UNIVERSITY OF KWAZULU-NATAL

COLLEGE OF LAW AND MANAGEMENT STUDIES,

SCHOOL OF LAW

THE EFFECTIVENESS OF THE E-COMMERCE LEGAL FRAMEWORKS IN SELECTED AFRICAN COUNTRIES

BY

MARYAM ADETOKUNBO ESANWA

(213571344)

Supervisor: Mrs. C.E Stevens

This Research Project is submitted in partial fulfillment of the regulations for the Master of Laws (LLM) in Business Law Degree at the School of Law at the University of KwaZulu-Natal

November, 2014.

DECLARATION

I, Maryam Esanwa, do hereby solemnly declare that:

(i) This thesis is my own original work, unless it is otherwise indicated.

(ii) This thesis has not been submitted for the purpose of fulfillment of any other degree or examination at any university except for the University of KwaZulu-Natal.

(iii) This thesis does not contain any other persons‘ writing, data, or other information, unless specifically acknowledged as being sourced from other persons. Where such sources have been quoted, then:

(a) Their words have been re-written but the general information attributed to them has been referenced;

(b) Where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

Signed

_____

Maryam A. Esanwa

ACKNOWLEDGEMENT

My profound gratitude goes to GOD almighty, most magnificent, ever benevolent, ever merciful, to whom alone, I owe everything, for His grace, mercies and favour upon me.

To my immediate family, consisting of my dear husband and best friend, Abdul Rahman, as well as our adorable daughter, Khadijah, thank you for being there for me, for your love, patience, motivation and encouragement, it means a whole lot to me.

My sincere gratitude goes to my parents - Dr. and Mrs. Esanwa, and my wonderful sisters for their love, support, prayers and admonitions over the years, and for their overwhelming support towards the realization of this achievement especially my mother, for the words of encouragement.

Last but not the least, my unreserved acknowledgement goes to my assiduous supervisor - Mrs C.E Stevens, I am thankful for your guidance, encouragement, support and inestimable contribution to the making of this work.

Thank you all.

TABLE OF CONTENTS

ABBREVIATIONS.

1. CMA – Computer Misuse Act, 1990.
2. COECC - Council of Europe's Convention on Cyber Crime.
3. E-Commerce – Electronic Commerce.
4. EDI - Electronic Data Interchange.
5. EEA – European Economic Area.
6. EFT- Electronic Funds transfer.
7. EFCC - Economic and Financial Crimes Commission.
8. E-mail – Electronic mail.
9. EU - European Union.
10. eUCP - Supplement to The Uniform Customs and Practice for Documentary Credits for Electronic Presentation.
11. EU Directive - European Union Directive on Electronic Commerce.
12. GUIDEC- General Usage for International Digitally Ensured Commerce.
13. IBLS - Internet Business Law Services.
14. ICC - International Chamber of Commerce.
15. IJLIT - International Journal of Law and Information Technology.
16. JDA- Journal of Developing Areas.
17. JICLT - Journal of International Commercial Law and Technology.
18. JILT- Journal of Information, Law and Technology.
19. Loy. L. Rev - Loyola Law Review.
20. MLEC- Model Law on Electronic Commerce, 1996.
21. MLES- Model Law on Electronic Signatures, 2001.
22. ₦ - Naira (The Nigerian Currency).
23. ODETTE - Organisation for Data Exchange by Teletransmission in Europe.
24. OHADA - Organisation for the Harmonisation of Business Law in Africa.
25. PELJ - Potchefstroom Electronic Law Journal.
26. POS - Point of Sale.
27. RICA - Regulation of Interception of Communications and Provision of Communications-Related Information Act.
28. SAJAAR - South African Journal of Auditing and Accountability Research.
29. SA Merc LJ – South African Mercantile Law Journal.
30. UNCECIC - United Nations Convention on the use of Electronic Communications in International Contracts.
31. UNCID - The Uniform Rules of Conduct for Interchange of Data by Teletransmission.
32. UNCITRAL - United Nations' Commission on International Trade Law.
33. WASET - World Academy of Science, Engineering and Technology.

TABLE OF CASES AND STATUTES

CASES

1. Anyaebosi v. R. T Briscoe Nigeria Ltd [1987] 3 Nigeria Weekly Law Reports 84 (part 59).
2. Anyaebosi v. R. T Briscoe Nigeria Ltd[1987] 3 Nigeria Weekly Law Reports 84 (part 59).
3. Douvenga R v. {District Court of the Northern Transvaal, Pretoria, case no 111/150/2003,19 August 2003(unreported case)}.
4. Georgia Dept. of Transportation v. Norris 1997. 474 S.E.2d 216 (Ga. App. 1996).
5. Goldblatt v. Fremantle (1920) AD 123, 128.
6. Jafta v. Ezemvelo KZN Wildlife(D204/07) [2008] ZALC 84; [2008] 10 BLLR 954 (LC); (2009) 30 ILJ 131 (LC) (1 July 2008).
7. Mashiyi S v and Another2002 2 SACR 387.
8. Ndiki S v. and others 2008 SACR 2 258.
9. Nuba Commercial Farms Ltd v NAL Merchant Bank Ltd & anor [2001] 16 NWLR 510 (part 740),
10. Nuba Commercial Farms Ltd v NAL Merchant Bank Ltd & anor[2001] 16 NWLR 510 (part 740).
11. Reid Bros (SA) Ltd v Fischer Bearings Co. Ltd (1943) AD 232 241.
12. Scherierhout v. Minister of Justice (1926) AD 99 109.
13. Uganda v Garuhanga and Mugerwa (CR 17 of 2004 Bugand Road Court).

STATUTES

- The Uncitral {United Nations‘ Commission on International Trade Law} Model Law on Electronic Commerce 1996 [MLEC].
- The Uncitral {United Nations‘ Commission on International Trade Law} Model Law on Electronic Signatures 2001 [MLES].
- The United Nations‘ Convention on the Use of Electronic Communications in International Contracts 2005 (UNECIC).
- The Supplement To The Uniform Customs And Practice For Documentary Credits For Electronic Presentation (Eucp) Version 1.1
- The Electronic Communications and Transactions Act (ECTA) (25 of 2002).
- Natal Law 12 of 1884; Act 68 of 1957; Act 71 of 1969; Act 68 of 1981.
- The Constitution of the Republic of South Africa, 1996.
- The Forgery and Counterfeiting Act 1981.
- Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002
- The Evidence (Amendment) Act, 2011.

- The Interpretation Act, Laws of the Federation of Nigeria, 2004.
- Advance Fee Fraud and other Fraud Related Offences Act 2006.
- The Constitution of the Federal Republic of Nigeria, 1999.
- The Bill for an Act to Provide for the Prohibition, Prevention, Detection, Response and Prosecution of Cyber Crimes and Other Related Matters 2013 (The Cyber rime Bill 2013).

CHAPTER ONE: INTRODUCTION TO ELECTRONIC COMMERCE[1].

1.1 Introduction.

The concept of trade has been in existence from time immemorial and has evolved from the traditional exchange of goods for goods (that is, trade by barter form), which was the starting point of what we know as trade today, to the exchange of goods for mediums of exchange, which serve as legal tender (that is, money)[2].

Moreover, the means of trading has equally evolved from the traditional face to face trading by means of paper documents, to a more advanced form of trading in which the buyer may never meet the seller, but would transact using paperless documents[3]. Presently, trade has evolved to encompass electronic processing and transmission of data, to include text, sound, picture and even video forms[4]. This has been made possible by the emergence of the internet[5].

Through the communication medium of the internet, businesses can reach customers who, otherwise, would never have known of the existence of certain products/services[6]. ‗The special nature of internet contracts has made most of the substantive rules applicable to commercial contracts inapplicable to such contracts'[7].

However, despite this apparently more convenient form of communication, many governments, internet users and business persons are generally confronted with a wide range of legal issues

---

[1] To be referred to as electronic commerce or e-commerce interchangeably during the course of the thesis.
[2] A Beattie, ‗The History of Money: From Barter to Banknotes', Investopedia online issue of 21 February, 2010 http://www.investopedia.com/articles/07/roots_of_money.asp, accessed on 5 March, 2014.
[3] F Le Roux, ‗E-Commerce: The Legal Framework' <http://butterworths.ukzn.ac.za/nxt/gateway.dll/zkfaa/bsxha/azjba/izjba/gwmba/pydua>, 1, accessed 1 March, 2013, 04:50pm.
[4] European Commission, ‗A European Initiative in Electronic Commerce', Communication from the Commission to the Council, The European Parliament, The Economic and Social Committee and the Committee of the Regions - Brussels, 16 April 1997, 157.
[5] AJ Kamssu, JS Siekpe & JA Ellzy, ‗Shortcomings to Globalisation: Using Internet Technology and Electronic Commerce in Developing Countries' (2004) 38 The Journal of Developing Areas, 151, 152.
[6] Ibid, 153.
[7] For instance, the determination of the exact moment when a contract can be said to have come into existence on the internet, giving rise to rights and obligations amongst parties in a contract is one of such complicated issues. TI Akomolede, ‗Contemporary Legal Issues in Electronic Commerce in Nigeria' (2008) 11 Potchefstroom Electronic Law Journal 1, 5.

as the existing legal rules do not always provide answers to the new issues that arise[8]. Hence, the need for Laws to fill the lacuna timeously, in order to inhibit legal uncertainty and prevent anarchy as regards e-commerce matters.

This thesis will explore the effectiveness of the e-commerce legal framework in certain African countries by using the United Kingdom‘s model of e-commerce regulation as a benchmark. This is proposed to be achieved by firstly embarking on an analysis of the concept of e-commerce. Secondly, this thesis will provide an overview of the historical development of e-commerce and its models. Lastly, this thesis will identify and critically analyse the benefits derived from it (e-commerce) as well as identify and discuss other issues relating to e-commerce.

Furthermore, an exploration of the existing international legal frame works regulating e-commerce will be undertaken. Thereafter, the existing laws and the methods of implementation in South Africa, Nigeria and the United Kingdom will be assessed in seriatim. In conclusion, a comparative analysis of the effectiveness of the various e-commerce legal frameworks in the selected countries will be undertaken. This is proposed to be achieved by first examining the prevalent legal frameworks in each of these countries. Subsequently, the merits and demerits of each of these Legal frameworks would be deduced, which would pave a way for recommendations to be proffered accordingly.

1.2 Rationale for the Study.

Our contemporary society has turned into one big global village, such that most transactions are being concluded by means of electronic commerce methods, which is fast becoming the norm in both developing and developed economies alike. There are multitudes of issues that have arisen and are still steadily arising as a result of this norm, such that it becomes pertinent to pose the question whether there exists a legal framework regulating such transactions and if it is indeed adequate to deal with the vast developments in this area of international trade law. In addition, one also has to consider the possibility of whether the developments in electronic commerce have outpaced existing laws in this area. If the answer to the latter question is

[8] Le Roux (note 3 above) 1.

affirmative, more so, there would be a need for a study that addresses these concerns and proposes sustainable measures to both countries and international bodies.

A worthy illustration of this study is the state of affairs on the African continent. An observation of Africa's Commerce reveals that the continent has witnessed a phenomenal growth in her internet usage over the past decade. As at 30th of December, 2000, the population of Internet users in Africa was 4,514,400, but by mid-2012 (30th of June thereof), the population had shot up to 167,335,676[9]. This shows a growth of 3,706.7 per cent[10]. Alongside the rise of African countries' participation in internet usage is a rise in the spate of cybercrimes in the continent[11]. The nature of such crimes and the lack of infrastructure and effective legal measure especially in African countries is sufficient reason for concerns.

This thesis is centered on international trade law and seeks to make an analysis of the electronic commerce related Laws in effect hinged on the UNCITRAL (United Nations' Commission on International Trade Law) Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures, or the lack of them. There are numerous articles discussing various aspects of Electronic Commerce, however, a good number of them seem to be outdated[12] and such articles appear not to cover the same field this research seeks to cover.

The aim of this work is to make a comparative analysis of the Legal regimes regulating Electronic Commerce in an African country which lacks a regulatory Legal framework (such as: Nigeria) with an African country which has implemented a Legal framework to regulate electronic commerce (such as: South Africa). Even more, the study aims to evaluate the situation in these countries vis-à-vis the situation in a developed country (the United Kingdom), which has a regulatory framework. This comparative analysis between the above

[9] Internet World Stats <http://www.internetworldstats.com/stats.htm> accessed 4th April, 2013.
[10] Internet World Stats <http://www.internetworldstats.com/stats.htm> accessed 4th April, 2013.
[11] P, Coetzer, _CyberCrime Escalates in South Africa, Losing the Global Battle against Online Fraud', April 19 2013 Leadership Magazine, accessed- http://www.leadershiponline.co.za/articles/cyber-crime-escalates-in-south-africa-6053.html, on 21 January, 2014, 04:27pm.
[12] Kamssu, Siekpe & Ellzy (note 5 above); Bamodu, 'Information Communications Technology and E-Commerce: Challenges and Opportunities for the Nigerian Legal System and the Judiciary', (2004) 2 The Journal of Information, Law and Technology (JILT). http://www2.warwick.ac.uk/fac/soc/law2/elj/jilt/2004_2/bamodu/; TI Akomolede, _Contemporary Legal Issues in Electronic Commerce in Nigeria' (2008) 11 Potchefstroom Electronic Law Journal 1, 8.

mentioned countries aims to seek a way forward for the particular African Countries under review, and by extension, Africa as a whole, by providing a viable proposal focused on equipping them to deal with the identified legal issues concerning e-commerce.

This issue is of academic and practical interest for a number of reasons which will be briefly provided. Firstly, only a number of African countries have implemented a Legal framework to regulate electronic commerce activities[13]. While other African Countries engage in electronic commerce activities unregulated[14]. Secondly, statistics reveal that cybercrime is growing faster in Africa than in any other continent, as 80 per cent of the personal computers on the continent are reported to be infected with malware[15].

Furthermore, the South African Cyber Threat Barometer 2012/13 puts the direct losses to cybercrime in South Africa between January 2011 and August 2012 at R2.65 billion, of which an estimate of R662.5 million was not recovered[16]. Cyber Crimes Watch reveals that 7.5 per cent of cyber-crime perpetrators are Nigerian[17], yet the existing laws in Nigeria are inadequate, as they simply cover issues relating to internet usage, but not the whole range of issues relating to cyber-crime[18], which are prevalent[19].

---

[13] ZN Jobodwana ‗E-Commerce and Mobile Commerce in South Africa: Regulatory challenges' (2009) 4 Journal of International Commercial Law and Technology, 1, 3.

[14] Ibid 3.

[15] PC Tools by Symantec, 14 October, 2010, <www.pctools.com/security-news/african-cybercrime/ > accessed 16 May, 2013. Malware is a general term used to refer to a host of hostile or intrusive software, deduced from the term ‗Malicious software'. It refers to software developed for the purpose of disrupting computer operation, gathering sensitive information or gaining access to private computer systems; examples include computer viruses, worms, Trojan horses, and spyware. See http://en.wikipedia.org/wiki/Malware, accessed on the 20th March, 2014.

[16] IT News Africa, 16th of May, 2013 < www.itnewsafrica.com/2013/01/south-african-cybercrimw-set-to-soar-in-2013/ > accessed on the 16th of May, 2013.

[17] Cyber Crimes Watch, 11th September 2011 < www.cybercrimeswatch.com/cyber-crime/cyber-crime-statistics.html > accessed on the 16th of May, 2013.

[18] E. Elebeke ‗Why cybercrime thrives in Nigeria by Ewelukwa' 13 April, 2011, Vanguard Newspapers < www.vanguardngr.com/2011/04/why-cyber-crime-thrives -in-nigeria-by-ewelukwa/ > accessed on the 16 of May, 2013.

[19] In Uganda, despite the enactment of relevant Cyber Crime Laws, a large majority fail to report incidences of cyber-crime to the relevant authorities. F. Tushabe & V. Baryamureeba ‗Cyber Crime in Uganda: Myth or Reality?' Proceedings of World Academy of Science, Engineering and Technology, ISSN 1307-6884, vol 8 (8 October, 2005) 68.

1.3 Research Problem and Structure of Thesis.

It appears as though some African countries have domesticated e-commerce related Laws[20], while many others have yet to domesticate their e-commerce Laws[21]. However, despite the domestication or otherwise, several African countries are faced with similar problems resulting from e-commerce, such as corruption[22], revenue losses[23] and cyber-crimes[24]. Thus, this thesis needs to investigate into the problems with the implementation of these provisions and find out why these countries are still struggling to come to terms with the basic electronic terms and provisions.

The key questions to be critically analysed throughout this research revolves around electronic commerce, especially in Africa. On the question of _what does electronic commerce mean and encompass?' this chapter of the thesis contains an in-depth explanation of the concept of Electronic Commerce. In a nutshell, electronic commerce encompasses _any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact'[25]. It also includes commercial forms such as Electronic Data Interchange (E.D.I)[26] and Electronic Funds Transfer (E.F.T)[27], as well as commercial

[20] For Instance, South Africa enacted the Electronic Communications and Transactions Act no. 25 of 2002, Zambia enacted the Electronic Communications and Transactions Act no 21 of 2009 and Uganda passed both the Electronic Signatures Act and Electronic Transactions Act of 2010 into Law, to mention a few. N. Ewelukwa, _Is Africa Ready for Electronic Commerce? A Critical Appraisal of the Legal Framework for ECommerce in Africa'< http://www.acicol.com/temp/Dr N.pdf > 1, 17.

[21] Such as Nigeria. Ibid, 18.

[22] P, Coetzer, (note 11 above), Milonics Analytics Blog, _Nigerian Banks Lose $260 Million to Cyber Crimes Says Central Bank of Nigeria', 23 June 2014, accessed http://www.milonics.com/blog/nigerian-banks-lost-260m-to-cybercrimes-says-central-bank-of-nigeria/, 18 October 2014, 6:16pm.

[23] A, Wakefields, _Cybercrime National Crisis Costing SA R1B a Year', Mail and Guardian issue of 23 October, 2013, accessed at http://mg.co.za/article/2013-10-23-cybercrime-costing-sa-r1b-a-year, on the 21 March, 2014 9:33pm.

[24] E, Okonji, _Nigeria: Report on Cyber Threat Calls for Quick Passage of 2012 Bill', This Day Online issue of 6 May 2014, accessed at http://allafrica.com/stories/201405080279.html, 20 October 10:29am.

[25] J Lourens, _Electronic Commerce, The Law and its Consequences' <http://butterworths.ukzn.ac.za/nxt/gateway.dll/zkfaa/bsxha/73dba/f4dba/6liba/pzeua> accessed 1st March, 2013, 04:50pm, 1.

[26] The concept of EDI will be discussed at length in chapter three, specifically under paragraph 3.4.1 below.

[27] EFT is a transaction that takes place over a computerized network, either among accounts at the same bank or to different accounts at separate financial institutions. In a nutshell, it facilitates the making of virtual payments into bank accounts, without the physical presence of the payer at a bank. Examples include: direct-debit transactions, wire transfers, direct deposits, Automated Teller machine (ATM) withdrawals and online bill pay services. Investing Answers, accessed at http://www.investinganswers.com/financial-dictionary/personal-finance/electronic-funds-transfer-eft-2328, on 19 November, 2014 12:45pm.

technologies such as Bar Coding[28], Electronic Imaging[29], Facsimile, E-mail, Internet Trade and Satellite Communications[30].

In addition, chapter two will provide a critical study of the benefits that are derived from Electronic Commerce. The research conducted this far has shown that the benefits derived from electronic commerce are numerous, and some of these include the fact that it is an expedient means of contracting, as it saves time and energy and that it is easily accessible[31].

In chapter three, international as well as national legal frameworks, will be explored. Some of the regulations governing E-Commerce transactions include:

i) The UNCITRAL {United Nations' Commission on International Trade Law} Model Law on Electronic Commerce 1996 [MLEC];
ii) The UNCITRAL {United Nations' Commission on International Trade Law} Model Law on Electronic Signatures 2001 [MLES];
iii) The Uniform Rules of Conduct for Interchange of Data by Teletransmission (UNCID);
iv) General Usage for International Digitally Ensured Commerce (GUIDEC); and
v) The European Union Directive on Electronic Commerce.

Each of these Legal instruments will be critically examined to derive a bearing on the extent to which they regulate E-Commerce activities in their domains of application. The examination of these legal instruments would serve to provide an explanation of the laws that are in place to regulate Electronic Commerce.

---

[28] A barcode is _a machine readable form of information on a scannable, visual surface' (also known as UPC codes). The barcode is read by using a special scanner that reads the information directly from it. In essence, barcoding refers to the technology employed in converting articles to become barcode sensitive. For instance, when purporting to purchase of an item at a store, the item is presented to a cashier, who seeks a label with thin, black lines across it, along with a variation of different numbers. This label is a barcode, which when scanned by the cashier, the item's description and price automatically come up. This technology is employed in achieving efficiency. National Barcode Website, accessed at http://www.nationalbarcode.com/articles/what-is-a-barcode.html, on the 19 November, 2014, 01:05pm.

[29] This refers to the technology employed in _using computer and/or specialized hardware or software to capture (copy), store, manipulate, process and distribute flat information such as documents, pictures, photographs, drawings and plans, through digitisation'. The Business Dictionary Website, accessed http://www.businessdictionary.com/definition/electronic-imaging.html, on the 19 November, 2014, 01:15pm.

[30] J Lourens, (see note 25 above) 1.

[31] S, Singleton & S, Halberstam: Business, the Internet and the Law, 1999, Trolley, London, 4.

Furthermore, the question of _How effective are these Laws, against the background of the economic realities in each selected country?' would be explored during the course of this research, in chapter four. This is proposed to be achieved via an analysis of the applicable laws in South Africa and Nigeria, in relation to the prevailing Law in the United Kingdom; against the background of their socio-political structures. Ultimately, chapter five will contain a comparative study of the Legal regimes in each of the countries under review, which will give rise to apposite recommendations being made, and a conclusion will be reached accordingly.

1.4 Objectives of the Study.

In relation to the objectives, the study will attempt:

- To define the concept of e-commerce;
- To analyse the benefits educed from electronic commerce;
- To embark on a study of some of the international legal regimes regulating e-commerce;
- To examine the legal regimes regulating e-commerce in certain African countries;
- To evaluate the efficacy of the legal regime in the selected African countries, against the background of their socio-political realities, via a comparative study with the United Kingdom;
- To make propositions relevant to the further development of e-commerce in Africa.

1.5 Literature Review.

Due to the unique nature of e-commerce, there appears to be a number of literatures on the topic of e-commerce. These writers' views will be used to address and analyse the research questions of the study. Furthermore, the study may utilize their work in the propositions for the further development of e-commerce in Africa.

One such author, Kamssu[32] discusses the concept of Electronic Commerce in view of developing countries at large. He traces the problems of access to internet technology to socio-

[32] Kamssu, (note 5 above); Bamodu, 'Information Communications Technology and E-Commerce: Challenges and Opportunities for the Nigerian Legal System and the Judiciary', (2004) 2 The Journal of Information, Law and Technology (JILT). http://www2.warwick.ac.uk/fac/soc/law2/elj/jilt/2004_2/bamodu/; TI Akomolede,

economic factors, by grouping countries as rich, mid-level economy and poor economy countries, and basing their level of assimilation of new technology according to the various groupings. He opines that the countries with the rich economy would be more engaged in the use of new technology, and by extension electronic commerce, much more actively than the latter groups. Kamssu makes a logical analysis of the problem by the use of hypothesis and statistics; however, the scope of his discovery covers a broader spectrum than this research work seeks to cover.

While Ewelukwa[33] analyses the issue of electronic commerce from the view point of Africa as a whole, by assessing the readiness of Africa to cater for the demands of e-commerce. He carefully analyses the Legal regime regulating Electronic Commerce in various African Countries, by identifying the various stages of implementation in these countries. In addition, he makes reference to the situation of non-implementation of a Legal framework for electronic commerce in Nigeria as _a rather disappointing case', in view of the fact that Nigeria is the most populous African country and has the highest population of internet users in Africa[34]. Once again, the scope of Ewelukwa's work exceeds the boundaries of this research, as this work is aimed at selected African countries, rather than Africa as a whole. Although, the learned author's work would provide useful reference for this thesis.

On the other hand, Jobodwana[35] engages with the concept of electronic commerce in relation to mobile commerce[36] within the context of South Africa only. He gives an account of the development of electronic commerce as well as m-commerce in South Africa, by making reference to the fore-runners in the industry as well as the progress made. The scope of Jobodwana's work pertains to only one aspect of the spectrum that this research seems to cover, as his article focuses on one country in particular (South Africa). In this sense, his work will be of value in analyzing the South African legal framework in e-commerce. However, this research will be anlsying two African countries and will aim to evaluate the efficacy of the

---

_Contemporary Legal Issues in Electronic Commerce in Nigeria' (2008) 11 Potchefstroom Electronic Law Journal 1, 8.

[33] Ewelukwa, (note 20 above).

[34] Ibid, 18.

[35] Jobodwana (note 13 above).

[36] To be referred to as m-commerce subsequently.

legal regime in these selected countries, against the background of their socio-political realities, via a comparative study with the United Kingdom.

With regards to the development of e-commerce Legislation, Gabriel[37] gives an account of the special nature of electronic commerce, while accentuating the need for its regulation, in order for it to yield more benefits than problems. He recounts the various legislations in existence to regulate Electronic Commerce in various developed countries like the United States of America[38], Canada[39], Australia[40] and several others, most of which were modeled against the background of the UNCITRAL {United Nations' Commission on International Trade Law} Model Law on Electronic Commerce 1996 [MLEC].

Gabriel discusses the salient provisions of the various Legislations regulating electronic commerce in various countries, identifies problems of electronic contracting and generally attempts at making recommendations based on the shortcomings identified in these Legislations. However, the aim of this work is focused on developing African countries, rather than developed Countries in general. But the legal framework in these countries could be of relevance to South Africa and Nigeria. Thus, despite the great deficit in development- a review of these countries' models may be of relevance in the development of a legal framework addressing the e-commerce needs of developing African Countries, which are yet to implement one, or the amendment, where necessary, for those who have implemented one.

1.6 Principal Theories upon which the Study will be based.

This research will be based on two main theories of International Trade Law. The first is the theory of comparative advantage. A country is said to have a _comparative advantage in the production of a good if it can produce such good at a lower opportunity cost than another country'[41]. This theory underscores the very essence of International Trade.

---

[37] HD Gabriel, _The Fear of the Unknown: The Need to provide Special Procedural Protections in International Electronic Commerce' 50 Loy. L. Rev. 307 2004, accessed at (http://heinonline.org) on Fri Mar 1 08:15:43 2013.
[38] The American Uniform Electronic Transactions Act, 1999.
[39] The Canadian Uniform Electronic Commerce Act, 1999.
[40] The Australian Electronic Transactions Act, 1999.
[41] L. Gonzalez, _The Theory of Comparative Advantage' (2004) <http://www.freerepublic.com/focus/f-news/1101717/posts> Posted on Saturday, March 20, 2004 5:54:53 AM, accessed 8 April, 2013, 9:51 am.

For instance, if country A and B are engaged in the production of two goods, country A is said to have a comparative advantage in the production of one of the goods (say cloth) if it can produce such a good at a lower opportunity cost than country B. The opportunity cost of producing this good by country A is defined as the amount of the other good (say wine) that must be given up by this country to produce one more unit of cloth. Thus country A would have a comparative advantage in cloth production relative to country B, if it must give up less wine to produce another unit of cloth than the amount of wine that country B would have to give up to produce another unit of cloth. This is regarded as the Comparative Advantage Theory.

Electronic Commerce can be used to provide market access for goods in African Countries at a minimal cost, such that they can effectively compete with the goods produced in other nations and at the same time, reap the benefits of Comparative Advantage, where an effective Legal framework exists to regulate electronic commerce.

The second theory is the Absolute Advantage Theory, which refers to the ability of a country to produce a product more efficiently than any other nation using the same amount or fewer resources[42]. This worthwhile objective can be facilitated by electronic commerce techniques, which are cost effective and time efficient.

Furthermore, the efficiency of goods produced in African Countries can also be accelerated by the presence of an effective Legal framework regulating electronic commerce in African Countries, such that producers in African countries are apprised of the existing standards for the nature of goods they produce, and aim at meeting such standards, with a lesser risk of fraud and the incidence of cybercrimes. When these standards are met, then such goods can effectively compete in the International market. This in turn increases the efficiency of the manufacturers in African Countries to produce goods, and by extension, they reap the benefits of the Absolute Advantage theory which in turn enables their economies to flourish.

[42] Ibid.

1.7 Research Methodology.

This thesis will be based on a desktop review of the relevant legal materials, by way of a qualitative review of the relevant literature (case law, international instruments, and national laws).

A study of certain prominent legal regimes currently in existence, such as the UNCITRAL Model Law on Electronic Commerce, UNCITRAL Model Law on Electronic Signatures and the domesticated version of these conventions in South Africa, with a view to ascertaining its impact on (developing) African countries. In addition, an analysis of the legal position as it pertains to e-commerce in an African country like Nigeria, which has failed to domesticate similar legislation, will be inquired into, in order to develop a well-supported research.

Furthermore, apposite cases will be referred to, in arriving at a conclusion on the true picture of electronic commerce in these selected African Countries and by extension- Africa as a whole.

1.8 Definitions and meaning of Electronic Commerce.

Electronic commerce is commonly known as ‗e-commerce' or ‗eCommerce'[43] and encompasses ‗any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact'[44]. It also means ‗doing business over the Internet, selling goods and services which are delivered offline as well as products which can be ―digitised" and delivered online, such as computer software'[45]. E-commerce can be thought of as a more advanced form of mail order purchasing through a catalogue, as almost any product or service can be offered via e-commerce[46].

In a broader sense, it includes commercial forms such as Electronic Data Interchange (E.D.I) and Electronic Funds Transfer (E.F.T), as well as commercial technologies such as Bar Coding, Electronic Imaging, Facsimile, E-mail, Internet Trade and Satellite Communications[47].

---

[43] http://www.investopedia.com/terms/e/ecommerce.asp, accessed on the 18th March, 2014, at 08:24pm.
[44] J Lourens,(note 25 above).
[45] ―Digitised" means the physical form of a good or service can be coded using digital technology and thereby distributed over the Internet. ‗E-Commerce Impacts and Policy challenges', a Publication of the Organisation for Economic Co-operation and Development (O.E.C.D), 2000, pg. 2.<www.oecd.org/eco/outlook/2087433.pdf>
[46] From books and music, to financial services, to plane tickets.
http://www.investopedia.com/terms/e/ecommerce.asp, accessed on the 18th March, 2014, at 08:24pm.
[47] www.oecd.org/eco/outlook/2087433.pdf.

_Modern e-commerce transactions typically use the World Wide Web at least at one point of the transaction's life cycle', although it may encompass a wider range of technologies, such as e-mail, mobile devices, social media or telephone[48].

A more comprehensive definition by the European Commission, which captures the multifaceted nature of E-Commerce, provides:

> Electronic commerce is about doing business electronically. It is based on the electronic processing and transmission of data, including text, sound and video. It encompasses many diverse activities including electronic trading of goods and services, online delivery of digital content, electronic fund transfers, electronic share trading, electronic bills of lading, commercial auctions, collaborative design and engineering, online sourcing, public procurement, direct consumer marketing, and after-sales service. It involves both products (e.g. Consumer goods, specialized medical equipment) and services (e.g. Information services, financial and legal services); traditional activities (e.g. Health care, education) and new activities (e.g. Virtual malls).

From the foregoing, it can be surmised that the scope of Electronic Commerce is wide. According to Kalakota and Whinston, it has been further defined to extend beyond all electronically mediated transactions relating to mere buying and selling, to encompass presale and post-sale activities[49].

1.9 Development of E-Commerce.

The concept of e-commerce as is known today was developed as far back as the late 1970s[50], and was known to encompass the electronic facilitation of commercial transactions using Electronic Data Interchange (EDI) and Electronic Funds Transfer (EFT) technologies, which allowed businesses to send invoices or purchase orders electronically[51]. In the subsequent years, e-commerce was known to encompass more things such as the Automated Teller Machine (ATM), credit cards and telephone banking[52].

---

[48] http://en.wikipedia.org/wiki/E-commerce, accessed on the 18th March, 2014, at 08:43pm.
[49] R Kalakota & A Whinston *Electronic Commerce A Manager's Guide*, 3 ed. Addison Wesley Reading (1997), 69.
[50] M, Aldrich, _The Inventor's Story, Aldrich Archive' (University of Brighton, 2008) <http://www.aldricharchive.com/inventors_story.html> (accessed 21 November 2013).
[51] A, Gib, _E-Commerce Development' http://www.articlesnatch.com/Article/A-Brief-History-Of-E-commerce/634686#.Uo4nxScgh9s (accessed 21 November 2013).
[52] Ibid.

However, the current constructs of e-commerce[53] did not arise until the pivotal year of 1990, when the first web browser program was written and the World Wide Web (www) was invented[54]. At this time (1990), commercial enterprise over the internet was strictly prohibited[55]. Several years later, security protocols allowing continuous connection to the internet were developed. Since the early 1990s, e-commerce had developed into the huge global internet market that exists currently, although, at this point, its function could be likened to that of a ‗glorified catalogue'[56]. However, by the beginning of the 21st century, more and more companies worldwide had begun offering their services over the internet, which had evolved from a passive marketplace to an interactive market offering a wide variety of items, which could be ordered for, paid for and sometimes, even delivered online[57].

At present, e-commerce allows consumers to exchange goods and services, while evading the age long barriers of time and distance[58] which served as a trade restriction. E-commerce has expanded rapidly over the last couple of years and it is predicted to continue at this rate or accelerate even further[59]. The ease with which e-commerce transactions are conducted and the speedy pace with which these transactions are concluded[60], amongst other factors have made e-commerce garner worldwide popularity.

Forrester research makes a projection to the effect that e-commerce retail sales in Western Europe will keep growing at an 11 per cent annual compound interest growth rate[61], while in the United States of America e-commerce retail sales will soar at this rate by 10 per cent

---

[53] As the ability to purchase a variety of goods and services over the internet using secure protocols and electronic payment systems.
[54] Aldrich (note 51 above).
[55] O A, Oduntan, ‗Taxation of Electronic Commerce: Prospects and challenges for Nigeria' 2010, electronic copy available at: http://ssrn.com/abstract=1697998, 1, 14
[56] Le Roux (note 3 above) 1. This was denoted by a shift from the use of catalogues for the advertisement of goods and services to the display of such goods and services on websites, as opposed to the interactive virtual interface that currently exists.
[57] Ibid.
[58] M, Roberts, ‗Ecommerce Development ' http://www.articlesnatch.com/Article/Ecommerce-Development/2635543#.Uo4nlScgh9s accessed 28th November, 2013, 05:16pm.
[59] Ibid.
[60] For instance, when a party uses a debit card to make a purchase at an online store, the transaction is processed using an EFT system. This results in an instantaneous payment to the merchant and a deduction from the party's bank account. This can be done anywhere the party is, saving transportation cost to a store and valuable time.
[61] E, Schonfeld, ―Forrester Forecast: Online Retail sales will grow to $250 billion by 2014", techcrunch.com 8th March 2010 issue, < http://techcrunch.com/2010/03/08/forrester-forecast-online-retail-sales-will-grow-to-250-billion-by-2014/ > , accessed 11th December 2013, 05:13pm.

between 2009 through till 2014[62]. Online retail sales in China are reported to have increased by 117 per cent between 2007 and 2009[63], and it is still on the rise. China currently boasts of an internet user base of over 420million[64]. Boston Consulting Group (BCG) projects that China will add an additional 30million users per year in the foreseeable future and by the year 2015 e-commerce would account for 7.4 per cent of the total retail sales[65].

1.10 E-Commerce Models.

E-commerce models can be broken into four major categories, namely- Business to Business (B2B), Business to Consumer (B2C), Consumer to Business (C2B), Consumer to Consumer (C2C)[66]. Other models include[67]- Government to Government (G2G), Government to important the research provides an explanation of these models.

1.10.1 Business to Business (B2B) Model.

This is an internet marketplace whereby exporters, traders, brokers, manufacturers, importers, wholesalers, retailers and other business communities from around the world meet for trade purposes[68]. As the name implies, this e-commerce model involves a transaction between business entities via the internet. Sometimes, companies which operate under the business to business model are virtual companies with no physical existence[69].

An example of this model can be found in the website[70]- www.amazon.com, which is an online bookstore that engages in the sale of books from various publishers. Here, the B2B model is at play, as each of the publishers has the option of developing a website through which they can advertise their books, yet, they transact with amazon for their books to be advertised on its website. It is important to note that the publisher represents a business entity, while amazon

---

[62] Ibid.
[63] A, Levitt, ‗China's booming E-commerce Market', 29th March, 2012, http://www.investopedia.com/stock-analysis/2012/chinas-booming-e-commerce-market-amzn-cqqq-ntes-wmt0329.aspx, accessed 20th March 2014, 08:30am.
[64] Ibid.
[65] Ibid.
[66] http://www.digitsmith.com/ecommerce-definition.html, ‗Ecommerce definition and types', accessed 22nd November, 2013, 02:37pm.
[67] Ibid.
[68] M, Roberts, ‗Ecommerce Development' http://www.articlesnatch.com/Article/Ecommerce-Development/2635543#.Uo4nlScgh9s accessed 28th November, 2013, 05:16pm.
[69] ‗Ecommerce Models' http://www.eservglobal.com/uploads/files/index.pdf, accessed 2nd December, 2013, 03:16pm.
[70] Ibid.

represents another business entity, therefore creating a classic case of the business to business e-commerce model.

It can be argued in favour of the Business to Business e-commerce model that it presents a cost-effective means of delivering specifically requested products while fostering efficiency.

1.10.2 Business to Consumer (B2C) Model.

This model is generally regarded as the most common E-Commerce model in use today[71]. It involves selling to the general public[72], usually in the form of a business transaction between a business entity or company and a consumer, such that the consumer deals with the manufacturer or retailer online in the purchase of goods and or services.

The Business to Consumer E-Commerce model applies to any business entity that sells its products online[73]. This includes online banking services, online shopping, travel services and even health services. The focus of the Business entities operating under this model of e-commerce is attracting and retaining customers, while at the same time ensuring profitability[74]. A classic example of the operation of the Business to Consumer Model of e-commerce in South Africa can be found at www.zando.co.za, which is a virtual store that sells a wide variety of clothes, shoes, accessories amongst other items from different brands.

The model operates as follows- products are advertised on the website in the form of an online catalogue, which contains details of the products, such as its availability, price, colours and other options. An interested buyer is expected to visit the website and place an order, while disclosing certain details such as size, colour, quantity and so on of the selected product(s), in such order. Upon placing an order, the customer is required to specify his personal and credit card details[75] on the website, which is verified and stored on Zando's database. Once the details are validated, the order is processed.

---

[71] Oduntan, (note 55 above) 15.
[72] _Ecommerce definition and types'(note 66 above).
[73] _Ecommerce Models' http://www.eservglobal.com/uploads/files/index.pdf, accessed 2nd December, 2013, 03:16pm. 2.
[74] Roberts, (note 68 above).
[75] The disclosure of such sensitive information on a website makes this model of ecommerce prone to security threats, and raises an issue of cybercrime, which is a major drawback to the development of ecommerce. _Ecommerce Models'(note 73 above) 3.

Against the background of the possible insecurity of personal and credit card information which customers are usually required to disclose under this model, it goes without saying that the business organisations have a great role to play in allaying the fear of customers in this regard by establishing reliable security measures[76]. As the success of E-Commerce lies in customers and merchants alike having the same level of confidence in purchase and sales transactions conducted over the internet, as that conducted at the mall, over the phone or via mail service[77].

The general idea of this model is that the business organisations target a large number of customers whom they offer their services to, record stupendous sales and at a minimal overhead cost[78]. As for the consumer, the advantage of this model lies in his liberty to shop at any time of the day, in the comfort of his home, while avoiding the crowd in the stores and have the items delivered at his doorstep[79].

1.10.3 Consumer to Business (C2B) Model.

This model simply involves a transaction being conducted between a consumer and a business entity[80], and is quite similar to the business to consumer model. However, the difference between this model and the business to consumer model lies in the fact that the consumer is regarded as the seller here, because he sets the price[81], rather than the business entity, which plays the role of a buyer.

[76] PS Bezuidenhout & JD Gloeck, _Identifying the risks in e-commerce payment for use by the IS Auditor', South African Journal of Auditing and Accountability Research (*SAJAAR)*, 4 (2003), 21-35, 21.
[77] Ibid, 21.
[78] A, Nickov, _eCommerce Business Models and Concepts',
http://www2.sta.uwi.edu/~anikov/comp6350/lectures/02-ECS-lect-eCommerce-business-models-concepts.pdf, accessed on 5th December 2013 at 10:54am, pg 8.
[79] Ibid.
[80] _Ecommerce Models' (note 73 above)4.
[81] Ibid 4.

In a nutshell, this model consists of individuals (or consumers) willing to offer products or services to, or be offered products or services by business entities[82]. Such individuals approach a website with a pool of target business organisations, on which they post the relevant information as regards such products or services including a price[83], by way of an advertisement. This advertisement operates as a form of invitation to treat. The result is that such organisations that are either in need of, or can provide the advertised products or services contact the consumer, by making an offer. The consumer is therefore at liberty to decide whether or not to accept the offer.

Here is a hypothetical example of how this model works- Mr. A (a consumer) has a project, which he seeks the services of a business organization to complete. He posts his project online, alongside a budget and other relevant information. Within hours he receives several bids for its completion. He thereafter reviews all the bids and decides on which business organization to appoint to complete the said project.

1.10.4 Consumer to Consumer (C2C) Model.

Any website which facilitates individuals being brought together to buy, sell or trade, is considered as operating a C2C E-commerce model[84]. This model affords consumers the opportunity of selling their personal assets, such as residential property, cars, motorcycles or even rent a flat by simply posting their information on a website[85].

A number of websites currently offer free classifieds, auctions and forums where individuals can trade freely[86] and make payments with the aid of mechanisms like paypal[87], through which

[82] http://www.tutorialspoint.com/e_commerce/e_commerce_business_models.htm, accessed 28th November, 2013, 3:47pm. Such services may include the comparison of car loan or personal loan rates online, the online sales of airline tickets, professional services and so on.
[83]Ibid.
[84] E-commerce webhosting guide < http://www.ecommerce-web-hosting-guide.com/ecommerce-business-models.html >, accessed 29th November, 2013, 8:51am.
[85]Note 82 above.
[86] http://www.digitsmith.com/ecommerce-definition.html, _Ecommerce definition and types', accessed 22nd November, 2013, 02:37pm. Examples of such websites include: www.ebay.com, www.gumtree.co.za, www.olx.co.za, and a host of others.
[87] This is a payment service which enables a person receive payment, pay for goods and send money without revealing his/her financial information, anywhere in the world. <https://www.fnb.co.za/downloads/PAYPAL-quick-guide-FNB.pdf> pg 2; see also https://www.paypal.com/webapps/mpp/buy.

money can easily be sent and received online. Other payment methods which may be employed include: Electronic Funds Transfer (EFT)[88], payment via credit cards or master cards and even payment on delivery[89].

A prospective seller visits a website operating the C2C E-Commerce model, posts his relevant information, consisting of the details of what he proposes to sell or the service he proposes to offer (as the case maybe) and a selling price at the very least. A prospective buyer visits the website, and if interested in any item for sale, bids for it or contacts the seller.

1.11 Conclusion.

E-commerce is at the centre stage of world commerce, such that no business unit can presently function without tapping into one form of e-commerce or the other[90]. This is the new norm, which appears like it is here to stay, going by its track record till date. It has several modes of application, and is steadily expanding. This calls for broad legislation to capture its complexities, and to offer certainty of the Law as regards e-commerce. Against the background of this introduction to the concept of e-commerce, a discourse on the intricacies of e-commerce is apposite. Chapter two below, would provide a broad analysis of the merits derivable e-commerce, issues pertaining to e-commerce and how these relate with the Law of contract.

[88] This encompasses an electronic exchange or transfer of money from one bank account to another, either within a financial institution or within multiple financial institutions, through computer based systems. <http://en.wikipedia.org/wiki/Electronic_funds_transfer>, accessed 18th December, 2013, 4:18pm.

[89] A number of E-Commerce online stores offer some, all, or more of these payment options, such as http://www.kinderelo.co.za

[90] By the use of a telephone, the internet, social media, e-mail.

CHAPTER TWO: ELECTRONIC COMMERCE

2.1 Introduction.

E-commerce has in recent years become an integral part of the multilateral trade system. One could almost draw the conclusion that the international trade would not be able to function without the basic elements entrenched in e-commerce. Therefore, the importance of e-commerce necessitates an understanding of the principles and its operation within the international and municipal legal frameworks. The obvious reason for this is that the system has a dual purpose- to ensure effective international operation and to enable relevant state parties to implement the framework within their municipal systems.

As alluded to in chapter one, e-commerce comprises _any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact'[91]. It encompasses the buying, selling and exchanging of products, services and information via computer networks, primarily the internet[92]. Over the years, e-commerce has steadily evolved into the position of the linchpin of modern commerce globally, serving as a medium through which businesses flourish. _E-commerce has allowed firms to establish a market presence or enhance an existing market position by providing a cheaper and more efficient distribution chain for their goods and services'[93].

The aim of this chapter is to critically analyse the benefits as well as those factors that ensure the successful operation of e-commerce. Firstly, the chapter will commence with identifying and then critically analyzing the benefits derived from e-commerce. Secondly, the chapter will focus on particular issues that are prevalent in e-commerce and then, will turn to focus on the demerits of e-commerce as well as the risks that the identified shortcomings pose. Furthermore, an exploration of certain mechanisms which may enhance the benefits of e-commerce, while at the same time, mitigate its disadvantages, such as legislations, will be undertaken thirdly. Fourthly, the nature of the traditional legal contract will be evaluated, as well as contracts involving e-commerce, highlighting the central theme - the benefits of e-commerce.

---

[91] Lourens, (note 25 above).
[92] Electronic Commerce, chapter 9, pg 274.
[93] http://www.investopedia.com/terms/e/ecommerce.asp, accessed on the 18th March, 2014, at 08:24pm.

2.2 Benefits Derived from E-Commerce.

Transacting business via E-Commerce is highly advantageous, owing to the instantaneous nature of business transactions of this form, which dispenses with the requirement of paperwork; hence, it saves time, while saving the environment[94]. Electronic commerce facilitates trade[95], as parties resident in opposite extremes of the world, effectively contract with each other without having to see each other[96], overcoming a trade barrier of distance. It also solves the problem of market access, as consumers in the remotest part of the world have access to goods, via the internet, which they would have ordinarily been unaware of[97].

The e-commerce platform creates a broader marketplace for buyers and sellers to meet, dispensing with the need for several personnel being employed to oversee the running of a business unit, hence, saving costs[98]; without limiting the number of transactions which could be carried on at a time, thereby fostering efficiency. The combination of these factors, amongst others, result in reduced cost of transaction savings, which could be passed on to the buyer in the form of low cost of goods and services[99]. A writer opines that the major significance of E-Commerce lies in the fact that it promotes a single world trading system, which is facilitated by access through electronic means, to goods and services all over the world[100]. While another writer holds the view that the internet (and by extension, e-commerce) ‗amounts to a technical improvement which lowers the costs of transaction, thus, generating far greater benefits than the triangular efficiency gains from trade liberalization'[101].

A further benefit of e-commerce exists in its speed, convenience and accessibility, 24 hours daily, weekdays, weekends and public holidays alike, as opposed to a standard business unit,

[94] A paperless method of transaction fosters an environmentally sound society, it substantially reduces the amount of trees to be fallen to produce paper, as the demand for paper is expected to reduce considerably. S, Singleton & S, Halberstam: ‗Business, the Internet and the Law', 1999, Trolley, London, p.4.
[95] As has been elaborated in the notes on e-commerce models above.
[96] D, Chaffey, E-Business and E-Commerce Management 2 ed. (Prentice Hall Harlow 2003), 16.
[97] There are several websites which provide this service to consumers, such as, www.ebay.com , www.kalahari.com, and a host of others.
[98] Chaffey (note 96 above) 16.
[99] Ewelukwa, (note 20 above) 5.
[100] Akomolede, (note 7 above) 8.
[101] A. Panagariya, ―E-Commerce, WTO and Developing Countries", the United Nations' Conference on Trade and Development, Policy Issues in International Trade and Commodities Study series 2, p.24.

which has a time constraint[102]. Surpassing the length of service customers receive at a traditional business outfit, while dispensing with the need of being physically present at the store and the possibility of having the goods delivered at their doorsteps. This is truly a convenient method of contracting! For instance, while a courier mail can take up to 12 hours to reach its destination, a long fax can take up to an hour to print at its recipient's premises; an e-mail can be received instantaneously by its recipient in a different time zone[103]. An e-mail has significant legal advantages over paper based methods of communication, and even far more over oral arrangements, for which a permanent record is often unavailable, whereas an e-mail automatically ensures record keeping, as it is difficult to fully delete[104].

In conclusion, from the above discussion, it is apparent that there are indeed benefits to e-commerce, which are advantageous to each participant in international trade. Since the research has identified the benefits of e-commerce, the focus will now turn to the issues concerning e-commerce.

2.3 Issues Relating to E-Commerce.

Despite the immense benefits e-commerce offers, as highlighted above, there are multitudes of issues (legal/procedural/normal business practice) inherent in its use, which range from means of proof of e-commerce transactions, to data protection, cyber-crimes and on to the issue of jurisdiction in the event of a dispute between the parties, amongst others. These issues bring to the fore the need for a Legal framework regulating e-commerce, which shall be discussed shortly.

2.3.1 Clear Identification of the Risks.

In as much as conducting business via E-Commerce has a plurality of benefits, as highlighted above, it is not without risks in itself. The legal risks of e-commerce are no greater than that associated with other means of contracting[105]. Its risks entail a combination of the traditional risks of sales and contracting, as well as new sets of risks related with electronic contracting[106].

---

[102] http://www.investopedia.com/terms/e/ecommerce.asp, accessed on the 18th March, 2014, at 08:24pm.
[103] Singleton & Halberstam (note 31 above) 4.
[104] Ibid 1.
[105] Ibid 1.
[106] Pacini C, Andrews C & Hillison W, _Legal Issues in Online Contracting: To agree or not to Agree' http://dx.doi.org/10.1016/S0007-6813(02)80009-X, accessed on the 25th April, 2013, at 11:39am, 1.

For instance, one of the most difficult issues regarding the use of the internet, and by extension, e-commerce contracting is the question of the applicable law in each transaction[107]. In addition to this, e-commerce transactions require compliance to a multiplicity of laws, as a webpage can be read in different states[108]; hence, the need to elaborate on these risks. Some of the risks alluded to include: jurisdiction, authentication and attribution, contract formation, contract validity, message integrity, non-repudiation and a host of others[109].

2.3.1.1 Jurisdiction.

Jurisdiction is a legal term used to describe the power or competency of a court to hear a dispute and decide disputes[110]. It can also be defined as the ‗power vested in a court to adjudicate upon, determine or dispose of a matter'[111]. In view of the global nature of E-Commerce contracting and due to its virtual form which enables it cross the barriers of territorial boundaries[112]; this tends to create confusion between parties in the event of a dispute, on the question of where the contract is formed and the applicable governing law.

Furthermore, each domestic court applies its internal procedural rules to determine the specific cases or instances in which it may have jurisdiction to resolve a dispute[113]. This situation however, breeds uncertainty as it makes the determination of jurisdiction in terms of an e-commerce contract difficult[114]. This is especially so, where it involves a contract concluded between parties of different nationalities. As a result, parties may have to grapple with a multiplicity of domestic procedural rules. This evinces a need for a unifying legal regime.

As far as internet contracts are concerned, and e-commerce, by extension, the general rule is that jurisdiction is determined by reference to the place or country where the contract is

[107] Singleton & Halberstam (note 31 above) 229.
[108] Ibid.
[109] Pacini, Andrews & Hillison (note 106 above) 2.
[110] S, Snail, ―Jurisdiction in Electronic Trans-Border Contracts" Kwazulu-Natal Law Society <https://www.lawsoc.co.za/default.asp?sl=&id=1888>, accessed on the 5th December, 2013 at 12:50pm.
[111] Ibid.
[112] Chaffey (note 96 above) 16.
[113] T, Rodriguez, ―Applicable Law and Jurisdiction in Electronic Contracts I" < http://www.emarketservices.com/clubs/ems/prod/E-Business%20Issue%20-Applicable%20law%201(1).pdf>, e-Business issue, December 2010, accessed on the 5th December, 2013, at 12:14pm, 2.
[114] Ibid 2-3.

performed[115]. Parties are encouraged to ‗ascertain the nature of their transactions from the point of inception of the contract'[116]. This would serve as a roadmap in the determination of what law governs, as well as what legal rights exist in each transaction. However, the virtual nature of internet contracts makes it difficult to determine where the parties are, when they are engaged in online dealings, especially with regard to goods deliverable online[117]. Consequently, it is difficult to characterize a contract as either international or domestic from the point of origination of the contract, much less determine jurisdiction. Nevertheless, this difficulty may be bridged if parties clearly state the governing law for their transactions in their contracts, or each party's domicile may be stated in the contract.

2.3.1.2 Contract Validity.

To start with, a contract has been defined as an agreement (arising from either legal or quasi mutual agreement) which is intended to be enforceable at Law[118]. The validity of an e-commerce contract would largely depend on the prevailing law in the country where the contract is performed and if such country has no defined e-commerce legislation, then, the basic rules of contract would apply[119]. The issue of contract validity is linked to jurisdiction.

It is important to note that the e-commerce technology has established a new form of contracting, different from the traditional method, given its ‗paperless' character. Hence, the virtual nature of e-commerce presents a dilemma of the Legal validity of a contract concluded via the web. The unique feature of this contract (e-commerce) makes one ponder whether contracts concluded over the internet are valid.

In South Africa, the Electronic Communications and Transactions Act[120] (ECTA) recognises any ‗data generated, stored, received, or sent by electronic form' to include ‗voice' and ‗a

[115] Davis O ―Contract Formation on the Internet: Shattering a Few Myths" in Edwards L and Waelde c (ed) Law and the internet, Hart Publishing Oxford (1997), 100.
[116] HD Gabriel, ‗The Fear of the Unknown: The Need to provide Special Procedural Protections in International Electronic Commerce' 50 Loy. L. Rev. 307-331, 2004, 326, accessed at (http://heinonline.org) on Fri Mar 1 08:15:43 2013.
[117] Ibid.
[118] Christie, RH ‗Law of Contract in South Africa', 3 ed (1996) 12.
[119] Van der Merwe, M & Janse van Vuuren, J, ‗Internet Contracts', pg. 156, accessed at http://www.legalnet.co.za/cyberlaw/cybertext/chapter6.htm, 12th December, 2013 at 6:27pm.
[120] Act 25 of 2002.

stored record'[121]. The Act gives legal effect to data messages and provides that information is not to be denied legal force and effect due to its form[122]. From these provisions we can deduce that the act provides for e-commerce transactions.

Furthermore, the ECTA substitutes certain criteria[123] for the validity of a legal contract, with such other criteria to suite the form of e-commerce techniques. It is important to state that certain contracts are required by law to be recorded in writing, to be registered, or to be notarially executed, such as contracts involving the sale of land, the assignment of a copyright or suretyship agreements[124].

For instance, the act substitutes the legal requirement of writing with the criteria that when the relevant information or document is in the form of a data message, and it is accessible in such a manner usable for future reference[125], then, the requirement of writing is deemed to have been met in respect of an e-commerce transaction. Section 12 provides as follows:

> A requirement in law that a document or information must be in writing is met if the document or information is -
> (a) in the form of a data message; and
> (b) accessible in a manner usable for subsequent reference.'

2.3.1.3 Contract changes and errors.

The effect of mistakes resulting from the transmission of messages by way of e-commerce methods need to be considered critically. If for instance, Mr. A and Mr. B contract via e-commerce means, and one of the parties' messages are intercepted by a third party, who includes terms in the agreement on Mr. B's behalf, which were not intended by Mr. B; Or where Mr. B mistakenly includes a term in the contract, which he did not intend. One has to consider what the (legal) consequence will be in the contract, as well as for the parties involved.

[121] Section 1 ECTA, definition of a Data Message. See Appendix A below for the specific provision of the ECTA.
[122] Section 11 ECTA.
[123] The criteria for the validity of a contract will be treated in a bit more detail below, under paragraph 2.3.3.2.
[124] Van der Merwe, M & Janse van Vuuren, J, Internet Contracts', pg. 156, accessed at http://www.legalnet.co.za/cyberlaw/cybertext/chapter6.htm, 12th December, 2013 at 6:27pm,156.
[125] Section 12 ECTA.

The United Nations Convention on the use of Electronic Communications in International Contracts (UNCECIC) establishes remedies in the case of ‗input errors by natural persons entering information into automated message systems'[126]. A solution to the interception of data messages by third parties may be available in the form of encryption[127] of data messages during transmission[128]. This provides some form of security, considering the fact that internet transactions are fraught with risks.

2.3.1.4 Authentication of Messages.

Authentication of messages refers to the technology which allows a party (the sender) to send a message to another (the receiver), in such a way that if the message is modified en route, the receiver would almost certainly detect it[129]. It protects the integrity of a message and ensures that each message received, is deemed to be accepted in the same condition as it was sent out, that is, with no bits inserted, missing or modified[130]. This raises issues as regards ascertaining the identity of the person with whom an agreement is purportedly being made. This particular risk involves identifying and developing methods to ensure the legitimacy of the content of messages received. It is against this background that the ECTA provides that where the signature[131] of a person is required, and no specific type of signature is specified, this requirement is deemed to be met if an Advanced Electronic Signature is used[132]. An Advanced Electronic Signature ‗means an electronic signature which results from a process which has been accredited by the authority as provided for in Section 37'[133].

---

[126] Article 14 UNCECIC.

[127] This is a cryptographic term, which means the process of encoding or conversion of data into a form, known as ‗a ciphertext', which cannot easily be understood by unauthorized persons. Accessed at http://searchsecurity.techtarget.com/definition/encryption on the 20th march, 2014, 12:23pm. Encryption does not serve as a bar to interception of messages, rather, it operates to reduce the likelihood of data messages being read by third persons.

[128] Bezuidenhout & Gloeck,(note 76 above), 23.

[129] M. Bellare & P. Rogaway: ‗Message Authentication', ch.7, pg. 1, accessed at http://cseweb.ucsd.edu/~mihir/cse207/w-mac.pdf, on the 21st of May, 2014 at 6:49pm.

[130] Ibid.

[131] A signature is a generally accepted means of authentication.

[132] Section 13 ECTA

[133] Section 1 ECTA. Section 37(2) ECTA provides that an Application to the Accreditation Authority must be made in the prescribed manner, supported by the prescribed information and accompanied by a non-refundable prescribed fee.

In addition, the identity information supplied by a correspondent in an e-commerce transaction may be used to identify such a person. This may be included in an e-mail, perhaps as part of the e-mail signature[134]. In the alternative, if the transaction involves the use of a website, a form requiring users to fill in specified identification details, may be attached[135].

2.3.1.5 Message Integrity.

Message integrity is concerned with the accuracy and completeness of a communication[136]. It also refers to the risk involved in being unable to detect whether the message received is actually what was sent by the other party. The ascertainment of the integrity of a message is critical to e-commerce, in terms of the negotiation and formation of contracts online, it is also relevant in terms of making electronic payments proving such transactions, using electronic records, if the need arises[137]. It therefore goes without saying that the consequences of a message being compromised may be fatal to any business concern. There are concerns about the form of e-commerce messages, where the message is sent without proper authentication methods. Such a situation leaves parties uncertain about the validity of the actual message received and the actual identity of the person(s) with whom they are contracting.

The ECTA tries to meet this requirement by means of a functional equivalence principle. This is to the effect that where the law requires for an information to be presented or retained in its original form, this requirement is met if the integrity of the information is ascertainable from the time it was produced in its final form and it is capable of being presented or produced in the presence of the person to whom it is to be presented[138].

2.3.2 Need for a Legal Framework.

The continued smooth running of human relationships is dependent on the existence of functional institutions, and as such relationships grow in number and complexity, so also must

---

[134] C, Reed: Internet Law: Text and Materials, Butterworths, London, Edinburg, Dublin (2000), p. 120.
[135] Ibid. An e-mail signature may consist of a name and /or other details written at the end of an e-mail, TJ, Smedinghoff & RH Bro, ‗Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce', 17 J. Marshall J Computer and Info. L. 723, (1999) at 730, accessed at http://repository.jmls.edu/cgi/viewcontent.cgi?article=1260&context=jitpl on 25th March, 2014.
[136] Yee Fen Lim: Cyberspace Law Commentaries and Materials, Oxford University Press, (2003), 220.
[137] Ibid, 220.
[138] Section 14 ECTA.

these institutions[139]. As stated earlier, e-commerce appears to be the new anchor of global commerce and has brought significant changes to world trade.

Considering the exponential growth of the internet, the question of whether or not to regulate it has been well mooted. It appears as though the majority of international organisations tend to have reached an accord on the need for a harmonized regulatory framework for e-commerce[140]. This has led to the promulgation of several model laws by the UNCITRAL, amongst similar bodies, as would be treated later in this paper. However, there are two distinctive features to be borne in mind as regards e-commerce, which set it apart from other methods of contracting. The first pertains to its largely unregulated nature, while the second touches on its face-paced nature which makes it almost impossible for the law to predict the next technology by making precognitive rules that reflect business practices using such new technology[141]. There are multitudes of issues that have arisen and are still steadily arising as a result of this new norm, it is therefore suggested that specific regulations addressing these issues resulting from the new electronic trading environment will significantly reduce the legal uncertainty e-commerce may raise and enhance the confidence with which the technology is employed.

In view of the risks presented by the use of E-Commerce, as discussed above, for any nation to maximize the benefits of E-Commerce, while protecting itself from the inherent risks, its implementation of a Legal framework to regulate E-Commerce activities is apposite. The existence of a Legal framework regulating E-Commerce is pertinent for the reasons below amongst others.

2.3.2.1 Exposure to the risks of E-Commerce.

Only a few African countries have implemented a Legal framework to regulate E-Commerce activities. While a larger majority of African Countries engage in Electronic commerce activities unregulated[142], and are exposed to the inherent risks unshielded, as will be discussed shortly. The following definition of the internet effectively captures the risk inherent in E-Commerce contracting – ‗A Net connection is a gateway to the external world, a doorway

[139] Yee Fen Lim (note 136 above)1.
[140] This is discussed in more detail in chapter 3.
[141] Gabriel, (note 37 above).
[142] IT News Africa, 16th of May, 2013 < www.itnewsafrica.com/2013/01/south-african-cybercrimw-set-to-soar-in-2013/ > accessed on the 16th of May, 2013.

through which anyone with Internet access can attempt to break into your internal computer system'[143]. According to the ECTA[144], _Internet means the interconnected system of networks that connects computers around the world using the TCP/IP and includes future versions thereof'.

The realization of the key merits of e-commerce, such as speed, efficiency and economy, require the recipients of data messages to act on such information upon receipt, timeously[145]. However, the indications of reliability associated with paper-based transactions[146] are replaced in e-commerce transactions with message authentication techniques; although, such techniques are not widely used. Moreover, the ease with which digital messages may be altered without detection, heighten the risk associated with this form of contracting[147].

In addition, when contracting by way of data messages, it is important to note that the traditional methods of verifying receipt of messages[148] do not apply. It is possible to verify that a message was received integrally in a point to point data communication, but there is no way of knowing precisely who the reply is coming from[149]. This in itself presents a risk. As Mr. A has no assurances that his message is being responded to by the intended recipient. This could have serious consequences for the parties if Mr. A's message is compromised. This paves way for the prevalent cyber-crime menace.

2.3.2.2 Cyber-crime.

Cyber-crime refers to any crime which involves a computer and a network[150]. Usually, a computer may either have been used in the commission of the crime or may be the target[151]. Dr. Halder and Dr. Jaishanker, give a comprehensive definition of cyber-crime as: _offences that

[143] TM Siebel & P House, Cyber Rules - Strategies for Excelling at E-business, Currency and Doubleday, May 1999. New York. 50.
[144] Section 1, ECTA.
[145] Smedinghoff & Bro, (note 135 above).
[146] Such as a signature in ink and delivery.
[147] Smedinghoff & Bro, (note 135 above).
[148] Such as proof of service of document(s), in the instance of court proceedings, which is usually a written document on which the recipient appends his signature. However, this mode is incongruent to e-commerce transactions.
[149] C, Vandenoever, _Information Protection, your Business and the Internet' , 1995 Deloitte &Touche LLP
[150] Moore, R Cyber Crime: Investigating High Technology Computer Crime, Cleaveland, Missisipi, Anderson Publishing (2005). The terms _Cyber-Crime' and _Computer crime' are used interchangeably.
[151] WG, Kruse & J.G Heiser, Computer Forensics: Incidents Response Essentials, Addison-Wesley, (2002), 392, ISBN 0-201-707 19-5.

are committed against individuals or a group of individuals with a criminal motive to intentionally harm the reputation of the victim or to cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks, such as internet (chat rooms, e-mails, notice boards and groups) and mobile phones (SMS/MMS)'[152].

Cyber-crime can be committed easily and anonymously, with a few resources, in a specific jurisdiction without the offender being physically present[153]. The fact that this crime can be committed without the perpetrator being physically present in his target area compounds the problem of detection[154]. Thus, the action of a perpetrator in country A, may have a direct and immediate effect on a victim in Country B[155]. In addition, the difficulty of proving who was at the keyboard in any given case accounts for the relatively low number of cyber-criminals successfully captured and punished[156].

Cyber-crimes pose many challenges to electronic commerce and have made internet transactions insecure and vulnerable to manipulation by persons who are not parties to such transactions[157]. It is also predictable that the proliferation of commerce on the internet will be

[152] D, Halder , & K, Jaishanker : _Cyber Crime and the Victimization of Women: Laws, Rights and Regulations', Hershey, PA, USA, IGI Global, 2011, ISBN 978-1-60960-830-9, accessed at http://www.igiglobal.com/?f, on the 21st March, 2014 at 04:10pm.

[153] MD Goodman & S Brenner _The emerging consensus on criminal conduct in cyberspace' 2002 *International Journal of Law and Information Technology*139–223 at 142, 146–150.

[154] F, Cassim, _Formulating Specialised Legislation to Address the Growing Spectre of CyberCrime: A Comparative Study' PER, vol 12, no. 4, 2009, pg.38.

[155] A case in point is that of the _love bug email virus' in May 2000, which was sent out in the form of an email, which replicated itself once opened and forwarded itself to all the email addresses of its victim. Once the virus becomes embedded on a host computer, it downloaded more dangerous software from remote websites, renamed files, extracted sensitive password protected information, redirected such information to certain websites and wiped out a good portion of information thereafter. It was reported that one tenth of the world mail servers were down on account of this virus which affected about 20 countries. Most unfortunately, the main person responsible for the creation and the spread of the virus was left unpunished as there were no computer crime related laws in his country, Phillipines, at the time of this event. They however promulgated a cyber-crimes related law in June of the same year, but cannot backdate the Law. See http://www.theguardian.com/world/2000/may/05/jamesmeek, http://nakedsecurity.sophos.com/2009/05/04/memories-love-bug-worm/, http://content.time.com/time/world/article/0,8599,2053699,00.html, accessed on the 20th March, 2014.

[156] L, Volonino, _Cyber Crimes', Salem Press Encyclopedia of Science, January 2013. Accessed at http://eds.b.ebscohost.com.ezproxy.ukzn.ac.za:2048/eds/detail?sid=6ad8038d-5ec0-4365-89ba-06abb49496b0%40sessionmgr115&vid=3&hid=115&bdata=JnNpdGU9ZWRzLWxpdmU%3d#db=ers&AN=89312105, on the 21st January, 2014, at 04:21pm.

[157] KG Akintola, RO Akinyede & CO Agbonifo: "Appraising Nigeria Readiness for E-Commerce towards achieving vision 20:2020" Nov. 2011 www.arpapress.com/Volumes/Vol9Issue2/IJRRAS_9_2_18.pdf 9.

matched by an expansion of crime on the internet[158]. The rise in the use of digital cash and credit cards over the internet provides a greater incentive to hack than ever before[159].

Conceptually, internet crime means the commission of unlawful acts using the computer, either as a tool or a target, or as both[160]. It encompasses e-mail scams, child pornography, hacking, data theft, extortion and a wide array of other nefarious activities[161]. The most common internet crimes include hacking, identity theft, the sale of illegal or stolen articles on the internet, phishing[162], and the creation of malicious codes such as viruses. These offences are crimes in most advanced countries because of statutory regulations. However, these activities are not crimes in a country which lacks legislation which clearly prescribes penalties for crimes[163].

Statistics reveals that cybercrime is growing faster in Africa than in any other continent, as 80 per cent of the pcs on the continent are reported to be infected with malware[164]. In South Africa for example, the country's Ombudsman for banking services avers that cybercrime is on the rise in the country. The Ombudsman's report reveals that in 2009, only 45 complaints of cyber-crime in the form of internet banking related fraud were received, however, by 2010, it had surged to 484[165]. This figure further escalated to 591 by the year 2011, and soared by a 3 per

[158]Ibid, 9.
[159] C, Gringas & N, Nabarro, The Laws of the Internet, Butterworths London (1977) 211.
[160]F, Cassim, "Formulating Specialised Legislation to Address the Growing Spectre of CyberCrime: A Comparative Study" PER, vol 12, no. 4, (2009) 36.
[161] AO Oyewunmi, : "The ICT Revolution and Commercial Sectors in Nigeria: Impacts and Legal Interventions", British Journal of Arts and Social Sciences, vol. 5, No. 2 2012,ISSN 2046-9578, accessed at http://www.bjournal.co.uk/paper/bjass_5_2/bjass_05_02_08.pdf, on the 4th March, 2013 at 06:12pm, 234-248, at 235.
[162] The term "phishing" refers to an e-mail scam that is sent to both consumers and companies in order to obtain either personal information from an individual or confidential information about an enterprise. The term was coined because phishers are "fishing" for personal information. For more information about phishing, see E Ryan Sunday Times "Ugly world of criminals who go phishing" 27 June 2010, 8.
[163] An instance in point is Phillipines before the promulgation of its cyber law, as discussed in note 155 above.
[164] PC Tools by Symantec, 14th October, 2010, <www.pctools.com/security-news/african-cybercrime/ > accessed on the 16th of May, 2013. Malware is a general term used to refer to a host of hostile or intrusive software, deduced from the term "Malicious software". It refers to software developed for the purpose of disrupting computer operation, gathering sensitive information or gaining access to private computer systems; examples include computer viruses, worms, Trojan horses, and spyware. See http://en.wikipedia.org/wiki/Malware, accessed on the 20th March, 2014.
[165]F, Cassim, "Formulating Specialised Legislation to Address the Growing Spectre of CyberCrime: A Comparative Study" PER, vol 12, no. 4, (2009) 42.

cent margin in 2012[166]. Furthermore, a news report reveals that the situation in the United Kingdom is not so different, as the number of online fraud incidents seem to be on the surge year on year[167]. These indicate the need for requisite measures alongside appropriate legislation to address this growing menace of cyber-crime.

2.3.2.3 Revenue loss[168].

The South African Cyber Threat Barometer 2012/13 puts the direct losses to cyber-crime in South Africa between January 2011 and August 2012 at R2.65 billion, of which an estimate of R662.5 million was not recovered[169]. Cyber-crime was reported to account for R1 billion yearly, on account of its ineffectual enforcement of Cyber laws[170]. Furthermore, it is reported by the United Kingdom's Commissioner that of all the frauds committed in Britain, 50 per cent was committed online (cyber-crime), costing the United Kingdom 70billion pounds a year[171]. This goes to show that it is not enough for an e-commerce legislation to be in place, an implementation mechanism is equally essential.

2.3.2.4 Inadequacy of existing Laws.

Every nation has a set of rules and regulations which govern it. However, e-commerce presents certain unprecedented situations which regular procedural rules do not apply to[172]. The inadequacy of these antiquated laws to address computer offences has led to the introduction of new legislation to deal with them[173]. Cyber Crimes Watch reveal that 7.5 per cent of cyber-crime perpetrators are Nigerian[174], yet the existing laws in this country are inadequate, as they simply cover issues relating to internet usage, but not the whole range of issues relating to

---

[166]Ibid.
[167] Ibid.
[168] It is estimated that the _love-bug e-mail virus' (discussed in note 155 above) caused damage in some 20 countries to the tune of $10 billion. http://www.wsws.org/en/articles/2000/05/bug-m10.html, accessed on the 21st March, 2014, 09:04pm.
[169] IT News Africa, 16th of May, 2013 < www.itnewsafrica.com/2013/01/south-african-cybercrime-set-to-soar-in-2013/ > accessed on the 16th of May, 2013.
[170] Wakefields (note 23 above).
[171] Coetzer, (note 165 above).
[172] For instance, the release of dangerous viruses which is done on the web can scarcely be charged by traditional laws due to the fact that this act is unlikely to be considered as a crime, except specialized legislation is made to this effect. Furthermore, the evidence of this act is incapable of meeting the evidential rules as regards originality.
[173]Cassim, (note 160 above) 42.
[174] Cyber Crimes Watch, 11th September 2011 < www.cybercrimeswatch.com/cyber-crime/cyber-crime-statistics.html > accessed on the 16th of May, 2013.

cyber-crime, which are prevalent[175]. Chapter five will provide a more detailed analysis of the issue.

2.3.3 Contracts.

By virtue of the Law[176] of contract, a contract can be defined as an agreement between two or more parties, with the intention that it is legally binding[177] and enforceable. For a contract to be enforceable, such a contract must consist of parties with legal capacity, the parties must be at a consensus on the terms of the contract, consideration must have moved from one of the parties to the other and the object of the contract must be for a legal purpose, as the law would not aid or uphold an illegality[178].

2.3.3.1 Formation of a Contract.

The general rule is that a contract is formed when parties reach an agreement on its terms, even orally[179] or by conduct[180], provided that the essential elements for the validity of a contract are met[181]. It is important to note that the Law requires certain agreements to be evidenced in writing[182], or to bear a signature[183] or that it be presented in its original form in order for it to be enforceable. In the context of E-Commerce however, the question ordinarily arises of whether a contract formed via E-Commerce means fulfills this requirement of writing, signature or originality.

---

[175] E. Elebeke ‗Why cybercrime thrives in Nigeria by Ewelukwa' 13th April, 2011, Vanguard Newspapers < www.vanguardngr.com/2011/04/why-cyber-crime-thrives -in-nigeria-by-ewelukwa/ > accessed on the 16th of May, 2013.

[176] The focus countries of this research -Nigeria, South Africa and the United Kingdom are common law jurisdictions, hence, operate similar legal systems.

[177] The Law Teacher, < http://www.lawteacher.net/contract-law/lecture-notes/agreement-lecture.php >

[178] Succinctly stated in other words by Innes CJ in *Scherierhout v. Minister of Justice* (1926) AD 99 109 thus: ―It is a fundamental principle of our law that a thing done contrary to the direct prohibition of the law is void and of no effect…"

[179] In the case of *Goldblatt v. Fremantle* (1920) AD 123, 128, Innes CJ held thus: ―Subject to certain exceptions, mostly statutory, any contract may be verbally entered into; writing is not essential to contractual validity." Culled from Christe RH, The Law of Contract in South Africa (2006) 5th ed. LexisNexis Butterworths, 105.

[180] *Reid Bros (SA) Ltd v Fischer Bearings Co. Ltd* (1943) AD 232 241.

[181] Such as Offer, Acceptance, Consideration and Intention to create Legal Obligations. See http://www.out-law.com/page-396, accessed 28 March, 2013, 08:45am.

[182] Such as contracts regarding alienation of land; suretyship contracts; credit agreements amongst others. See from Christe, (note 179 above) ch. 3, 105-129.

[183] Section 1 of the Natal Law 12 of 1884, which was repealed and replaced by Section 1 of Act 68 of 1957, and then repealed and replaced by Act 71 of 1969 and then Section 2(1) of the Act 68 of 1981 provides thus: ‗No alienation of land after the commencement of this section shall…be of any force or effect unless it is contained in a deed of alienation signed by parties thereto or by their agents acting on their written authority.'

2.3.3.2 Validity of a Contract.

By virtue of the provision of Article 11 of the UNCITRAL MLEC[184], the expression of an offer and the unequivocal acceptance of an offer between parties to a contract by means of data message(s) are valid and enforceable. As regards the point in time in which an E-Commerce contract is deemed to be formed, Article 15(1) of the UNCITRAL MLEC provides that the dispatch of a data message[185] occurs at the time when it enters an information system outside the control of the originator; while an addressee is deemed to have received a data message when the complete data message has entered an information system of the addressee / at the time when the message is retrieved by the addressee[186].

On the other hand, a data message is deemed to be dispatched at the originator‘s place of business or residence, and receipt is deemed to take place at the addressee‘s place of business or residence[187]. This means that for the purpose of determining the origin of a data message, the sender‘s place of business or residence is instructive. Conversely, the recipient‘s place of business or residence is deemed to be the destination of a data message, despite its virtual form.

2.3.3.3 How do we deal with the requirement of writing in E-Commerce?

As stated above, the Law requires certain documents to be evidenced in writing, without which it is not considered valid. The question arises whether a contract concluded via e-commerce means fulfills this requirement of writing. There are divergent views on this point[188]. The Supreme Court of Nigeria‘s decision in *Anyaebosi v. R. T Briscoe Nigeria Ltd*[189] is in conflict with the Nigerian Court of Appeal‘s decision in ***N****uba Commercial Farms Ltd v NAL Merchant*

[184] The UNCITRAL {United Nations‘ Commission on International Trade} Model Law on Electronic Commerce 1996 [MLEC], hereinafter referred to as UNCITRAL MLEC.

[185] Article 2 of the UNCITRAL MLEC defines a data message as ~~in~~formation generated, sent, received or stored by electronic, optical or similar means, including but not limited to Electronic Data Interchange (EDI), Electronic Mail, telex or telecopy”.

[186] Article 15(2) of the UNCITRAL MLEC.

[187] Article 15(4) of the UNCITRAL MLEC.

[188] A 1997 court ruling by a Georgia Appellate court has contributed to this uncertainty. In *Georgia Dept. of Transportation v. Norris* , 1997. 474 S.E.2d 216 (Ga. App. 1996), reviewed on other grounds, 486 S.E.Zd 826 (Ga.) the court held that filing a notice by fax did not satisfy a requirement that notice be in writing because the transmission of ~~b~~beeps and chirps” along a telephone line is not writing in the customary sense of the term.

[189] [1987] 3 Nigeria Weekly Law Reports 84 (part 59).

Bank Ltd & anor[190], on the issue of the admissibility of Computer print outs as evidence, the Court of Appeal was of the view that the Evidence Act (s. 97) only provides for the admissibility of evidence in ‗book' form, and accordingly, held that computer printouts were inadmissible.

While in South Africa, a look at earlier case law evinces the need for specific legislation for the regulation of e-commerce transactions. The case of *S v Mashiyi and Another*[191] is a case in point where the question of admissibility of computer-generated documents arose. The court held that in terms of the ‗prevailing law', it could not admit the disputed documents which contained information that has been processed and generated by a computer into evidence[192]. Recent case law in South Africa shows that the Labour Court now recognizes the validity of a contract concluded by mail and text messaging as satisfying the requirement of writing in the decided case of *Jafta v. Ezemvelo KZN Wildlife*[193].

However, the UNCITRAL MLEC has purported to solve this problem of divergent rulings as regards the admissibility or otherwise of a data message as a result of its form, as seen in the rejection of fax messages and computer print outs above, simply because they do not appear in the traditional written form, by redefining the concepts of writing, signature and originality to accommodate modern E-Commerce methods, such as electronic mails, telex and a host of others[194], while establishing criteria for their authenticity, to achieve uniformity as regards E-Commerce.

2.3.3.4 How do we deal with the requirement of Signatures in E-Commerce?

The UNCITRAL MLEC, in Article 7 deals with the issue of signatures, it provides:

> (1) Where the law requires the signature of a person, that requirement is met in relation to a data message, if:

[190] [2001] 16 NWLR 510 (part 740).
[191] 2002 2 SACR 387.
[192] Cassim, (note 173 above) 127.
[193] (D204/07) [2008] ZALC 84; [2008] 10 BLLR 954 (LC); (2009) 30 ILJ 131 (LC) (1 July 2008). This case was decided based on the South African Electronic Communications and Transactions Act, 2002.
[194] See note 83 above.

(a) A method is used to identify that person and indicate that person's approval of the information contained in the data message; and

(b) The method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

In essence, an electronic signature is deemed to have the same status as a hand written signature if a method is used to identify the person and indicate his approval of the message and if the method used for its authentication is reliable and appropriate for the purpose for which the data message was created, in the light of surrounding circumstances[195]. The UNCITRAL Model Law of Electronic Signatures (MLES), 2001 builds further on the principle laid down in Article 7 of the UNCITRAL MLEC.

The underlying objective of the MLES, as may be deduced from the provisions, is the creation of functional legal equivalence between traditional means of signing or authenticating documents and electronic techniques[196]. Both Digital Signatures based on cryptography (such as public key infrastructure) and Electronic Signatures using other technologies are recognised by the MLES. Article 6 of the UNCITRAL MLES establishes the criteria for determining the reliability of an electronic signature used. This issue would be discussed further in chapter three.

2.4 Conclusion.

Despite the benefits of e-commerce highlighted above, it is clear that e-commerce methods vary from its paper-based alternatives. Although the UNCITRAL model laws attempt at encouraging the implementation of legislation equating e-commerce with the traditional modes, the risks inherent in e-commerce methods still thrive. Going by the above discourse, it is apparent that e-commerce is a highly advantageous means of transacting, but is not without its shortcomings. Furthermore, a legal framework for the regulation of e-commerce transactions is pertinent for the maximization of the benefits of e-commerce, while minimizing its disadvantages to the barest minimum. In addition to a regulatory framework, an

[195] Article 7, MLEC.
[196] The World Trade Organisation (WTO) website <http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html>, accessed on the 8th of March, 2013, at 03:59pm.

implementation mechanism to ensure its efficiency is also relevant to complement such regulation.

CHAPTER THREE: THE INTERNATIONAL LEGAL FRAMEWORK FOR E-COMMERCE.

3.1 Introduction.

A major challenge which has accompanied e-commerce since its inception is the task of regulation. This challenge is heightened by the virtual nature of e-commerce and its ability to break down physical barriers by seemingly crossing borders. Various institutions and organisations have attempted at surmounting this challenge, by the creation of regulatory frameworks to govern domestic and international e-commerce transactions. Such institutions as the International Chamber of Commerce (ICC), the International Institute for the Unification of Private Law (UNIDROIT), the Comite Maritime International (CMI), the United Nations' Commission on International Trade Law (UNCITRAL), the Organisation for the Harmonisation of Business Law in Africa (OHADA) and the European Union (EU) have all made concerted efforts in this regard. Such efforts have yielded in a number of the harmonized Legal regimes regulating e-commerce over the years, which include:

- The Hague & Hague-Visby Rules, 1978, developed by the CMI;
- The United Nations' Convention on Contracts for International Sale of Goods, 1980;
- CMI Rules for Electronic Bills Of Lading, 1990;
- The UNCITRAL {United Nations' Commission on International Trade Law} Model Law on Electronic Commerce 1996 [MLEC];
- The UNCITRAL {United Nations' Commission on International Trade} Model Law on Electronic Signatures 2001 [MLES];
- The United Nations' Convention on the Use of Electronic Communications in International Contracts 2005;
- The United Nations' Convention On Contracts For The Carriage Of Goods Wholly / Partly By Sea, 2008;
- The Supplement to The Uniform Customs and Practice for Documentary Credits for Electronic Presentation (eUCP) version 1.1, developed by the ICC.

The international Legal regimes currently regulating e-commerce are the key focus of this chapter. The following conventions/legal instruments would be discussed in more detail below:

- The Uniform Rules of Conduct for Interchange of Data by Teletransmission (UNCID);
- General Usage for International Digitally Ensured Commerce (GUIDEC); and
- The European Union Directive on Electronic Commerce.

However, the key International instruments of interest to this discourse are the UNCITRAL Model Law[197] on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures. This thesis concentrates on these instruments on account of the fact that these model laws are the key universal instruments which have been specially formulated to address e-commerce issues across the globe and form the backbone of most e-commerce legislations all over the world. In a nutshell, the peculiar features inherent in them as well as their wide application account for the interest of this thesis in the Model Laws. The aims of these Model laws include the unification of rules to make room for the acceptability of paper-based documents.

Both Model Laws are based on the Fundamental Principles of non-discrimination, technological neutrality and functional equivalence[198]. In respect of non-discrimination, the Model Laws impart legal recognition to data messages, by ensuring that a document is not denied legal effect, validity or enforceability, solely on the grounds of its electronic form[199]. This, in effect, removed some of the obstacles which prevented the wide acceptability of electronic messages and documents.

In terms of technological neutrality, the model law mandates the adoption of provisions that are neutral, with respect to the technology used, with the aim of accommodating any future development without further Legislative work by the adopting country. A key impediment to the acceptability of new technologies, such as electronic messages is that at the time majority of existing legislations were drafted, these technologies were not pre-empted, as they were not

[197] A Model Law does not have the same legislative weight as a convention, and perhaps does not bring the same level of unification, but it does away with many of the delays and bureaucratic measures associated with conventions', Indira, C: International Trade Law, (2005), 3rd ed, Cavendish Publishing Limited, p.109.
[198] The WTO website, (note 196 above).
[199] Article 5, UNCITRAL {United Nations' Commission on International Trade} Model Law on Electronic Commerce 1996 [MLEC].

in existence, and when they came into existence they tend to be treated with uncertainty, until legislations are made as regards them[200]. However, against the background of this trend, the model laws attempt at overcoming similar hurdles by this feature of technological neutrality.

While the principle of functional equivalence analyses the purposes and functions performed by the traditional paper-based requirements, with a view to determine how these functions and purposes can be achieved by e-commerce techniques. For instance, the principal functions of a signature are to identify the signatory and to ascertain the signatory's consent to the content of a document. The position of the Model Law is that once an electronic message successfully fulfills these functions, then it is regarded as legally acceptable as a signed document[201]. Hence, the requirements of original, signature, and so on are met using electronic techniques.

It is important to note that the UNCITRAL Model Laws are intended to serve as a guide for domestic legislatures to _update their legislation' in order to incorporate e-commerce into their national Laws on contracts[202].

3.2 The UNCITRAL Model Law on Electronic Commerce {MLEC}.

This Model Law was adopted in 1996, with a view to establish a common legal framework among nations in order to impart legal certainty by way of a flexible approach. The focus of this Law was on the requirement of writing and signatures for the purpose of validity and enforcement of a contract. The Model Law was published along with a guide to its enactment, with the intention that it be used as an aid in its interpretation, to ensure a uniform approach.

The MLEC establishes rules for the formation and validity of contracts concluded by electronic means, for the attribution of data messages, for the acknowledgement of receipt and for the

[200] _An Introduction to Interchange Agreements', accessed at http://www.unece.org/tradewelcome/areas-of-work/un-centre-for-trade-facilitation-and-e-business-uncefact/outputs/standards/unedifact/tradeedifactrules/part-2-uniform-rules-of-conduct-for-interchange-of-trade-data-by-teletransmission-uncid/part-2-uncid-chapter-4-annex.html on the 13th May, 2014, at 07:14pm.
[201] Sax, M: _International Law Issues Relating to Electronic Commerce', 2001, accessed at http://saxlaw.com/publications/ELECTRONIC_COMMERCE.html on the 17th, May, 2014 at 12:35pm.
[202] Lisandro A. Allende & Mariana A. Miglino, Internet Law - International Electronic Contracting: The UN Contribution, Internet Business Law Services (IBLS) Internet Law - News Portal, Mar. 6, 2007, http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1610 (last visited 26 November, 2014).

determination of the time and place for the dispatch and receipt of data messages[203]. The salient features of the Model Law will be discussed further in the course of this work.

3.2.1 Key features of the UNCITRAL Model Law on Electronic Commerce {MLEC}.

To start with, the UNCITRAL Model Law purports to enable and facilitate Commerce conducted using electronic means, focusing on the requirement of writing and signatures for the purpose of removing the legal obstacles arising from statutory provisions and increasing legal predictability for e-commerce[204]. Furthermore, the model Law attempts at providing ‗equal treatment to paper-based and electronic information', to enable its use and foster efficiency in international trade[205].In addition, it embodies the most definitive treatment of issues regarding international electronic commerce[206].

3.2.2 Scope of the MLEC.

The MLEC applies to commercial activities, which include ‗Sales, Factoring, Agency Agreements, Distribution Agreements, Leases, Industrial Co-operation and transportation of goods by air, rail, sea or road'[207]. In the context of the UNCITRAL MLEC, information within the meaning of e-commerce is regarded as a data message[208]. While *Article 5 of the UNCITRAL MLEC* gives Legal effect to a data message, in providing that ‗a data message shall not be denied effect solely by reason of its form'. This relates the principle of non-discrimination against a document by denying its admissibility as evidence due to its outlook or form.

The information in a data message is deemed to have met the requirement of writing if it is accessible subsequently[209]. *Article 6 MLEC* provides: ‗Where the law requires information to be in

[203] Article 15 UNCITRAL MLEC.
[204]< http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/1996Model.html> accessed on the 8th of March, 2013 at 03:59pm.
[205] Ibid.
[206] Introduction to GUIDEC II, The International Chamber of Commerce website, accessed at http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2001/GUIDEC-General-Usage-for-International-Digitally-Ensured-Commerce-(Version-II)-01/10/2001/, on the 13th May, 2014 at 12:29pm, pg. 7.
[207] Article 1, UNCITRAL MLEC.
[208] Article 2 of the UNCITRAL MLEC defines a data message as ―information generated, sent, received or stored by electronic, optical or similar means, including but not limited to Electronic Data Interchange (EDI), Electronic Mail, telex or telecopy".
[209] Article 6 UNCITRAL MLEC.

writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference‘.

This is a demonstration of the functional equivalence feature at play, as the key function of a written document[210] is its availability to be referred to, when the need arises. Provided that this need is fulfilled, the MLEC deems the requirement satisfied, irrespective of the form (tangible or intangible) of the document concerned.

Furthermore, where a method is devised to identify a party to a contract and confirm the party‘s approval of the information contained in a data message and such method is found to be reliable for the purpose for which the data message was created, in the light of surrounding circumstances, the requirement of signature is deemed to be met in relation to a data message[211]. This provision is an indication of a reflection upon the role of a signature in constituting a binding contract, in the sense that it identifies the signer and indicates his assent to the signed document. The MLEC however, does not specify what method of signing a data message is appropriate and under what circumstances[212]. The guide to the MLEC suggests that it may be useful, in the context of data messages to _develop functional equivalents for the various types and levels of signature requirements in existence‘[213]. This is somewhat open-ended in the sense that certain aspects, like this, are not specifically legislated upon to give room for adopting countries to fill the gaps[214].

In addition, the requirement of originality is met by a data message, where the law requires information to be presented or retained in its original form, if:

---

[210] Some of the functions of a paper document are highlighted in the Guide as follows: i) to provide a document that would be legible by all; ii) to provide a document that would be unalterable over a period of time; iii) to allow for the reproduction of a document, such that each party would have a copy of the same document; iv) to allow for the authentication of data by means of signature and v) to provide for a document acceptable to courts and public authorities. The UNCITRAL MLEC and Guide to enactment, para 16 of the Guide, accessed at http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf, on the 10th of July, 2013, at 10:15am.

[211] *Article 7 UNCITRAL MLEC.* This requirement seems to be somewhat vague. Its provision has been reviewed by the provision of *Article 6 of the UNCITRAL MLES*, to be discussed below.

[212] Introduction to GUIDEC II, The International Chamber of Commerce website, accessed at http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2001/GUIDEC-General-Usage-for-International-Digitally-Ensured-Commerce-(Version-II)-01/10/2001/, on the 13th May, 2014 at 12:29pm, pg. 7.

[213] The UNCITRAL MLEC and Guide to enactment, para 55 of the Guide, accessed at http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf, on the 10th of July, 2013, at 10:15am.

[214] The Model Law is actually drafted as _an open-ended instrument to be complemented by future work‘, as was alluded to, in its guide. The UNCITRAL MLEC and Guide to enactment, para 11 of the Guide, accessed at http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf, on the 10th of July, 2013, at 10:15am.

a) ‗there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and
b) where it is required that the information be presented, and that information is capable of being displayed to the person to whom it is to be presented'[215].

The twin values of integrity and reliability are apposite to establishing the originality of a data message, and are addressed in *Article 8(3)*. This article provides that the criteria for assessing integrity are ‗whether the information has remained complete and unaltered'[216]. While ‗the standard for reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all surrounding circumstances'[217].

On the other hand, the issue of the admissibility of computer generated evidence is a chief cause of uncertainty as regards e-commerce transactions. This issue, alongside the evidential weight of data messages is squarely addressed in *Article 9. Article 9(1)* sets out the non-discrimination against data messages, by virtue of their form. It states that data messages should not be denied admissibility in evidence solely on the grounds that it is a data message or that it is not in its original form[218]. It provides further, that:

> In assessing evidential weight of a data message, regard shall be had to:
>
> i) the reliability of the manner in which the data message was generated, stored or communicated;
> ii) the reliability of the manner in which the information was maintained;
> iii) the manner in which the originator was identified; and
> iv) any other relevant factor[219].

Having taken a cursory look at salient aspects of the MLEC, this leads us to an overview of the relevant provisions of the MLES.

[215] Article 8(1) UNCITRAL MLEC.
[216] Article 8(3)(a) UNCITRAL MLEC.
[217] Article 8(3)(a) UNCITRAL MLEC.
[218] Article 9(1)(a)&(b) UNCITRAL MLEC.
[219] Article 9(2) UNCITRAL MLEC.

3.3 The UNCITRAL Model Law on Electronic Signatures, 2001[220](MLES).

The purpose of this Model Law is to enable and facilitate the use of Electronic Signatures by establishing criteria of technical reliability for the equivalence between electronic and hand-written signatures. It serves as a benchmark for states seeking to establish a modern and harmonized Legal framework to effectively address the Legal treatment of E-Signatures and impart on it the status of Legal certainty[221]. This Model Law has been described as a demonstration of an emerging international consensus on the use of authentication/certification/standardized schemes to determine enhanced legal effect[222].

3.3.1 Key features of the UNCITRAL MLES.

Firstly, the MLES lays down basic rules of conduct for assessing the duties and liabilities of the parties to a contract dealing with Electronic signatures. Secondly, it contains provisions that underscore its principle of technological neutrality, amongst other principles, by establishing equal treatment for signature technologies[223]. Lastly, the MLES provides specific rules of conduct for the signatory, the service provider and the relying party and holds the parties responsible for failure to satisfy the requirements[224].

3.3.2 Scope of the UNCITRAL MLES.

The provision of *Article 6 of the UNCITRAL MLES* is of relevance to this discourse. This article builds upon the provision of *Article 7 of the UNCITRAL MLEC*, which provides that where a method is devised to identify a party to a contract and confirm the party's approval of the information contained in a data message and such method is found to be reliable for the purpose for which the data message was created, in the light of surrounding circumstances,

---

[220] Adopted on the 5th of July, 2001, with a guide to its enactment. <http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html> accessed on the 15th of July, 2013.
[221] Ibid.
[222] C.Kuner, R.Barcelo, S.Baker & E.Greenwald: _An Analysis of International Electronic and Digital Signature Implementation Initiatives' Internet Law and Policy Forum, accessed at
[223] Article 3, UNCITRAL MLES.
[224] Introduction to GUIDEC II, The International Chamber of Commerce website, accessed at http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2001/GUIDEC-General-Usage-for-International-Digitally-Ensured-Commerce-(Version-II)-01/10/2001/, on the 13th May, 2014 at 12:29pm, 8.

then, the requirement of a signature is deemed to be met in relation to a data message[225]. However, in addition to this, *Article 6 of the UNCITRAL MLES* imposes the following conditions to establish the reliability of a signature:

> (a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;
> (b)The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
> (c)Any alteration to the electronic signature, made after the time of signing, is detectable; and
> (d)Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable[226].

It is important to note that all the above conditions must be met for the establishment of the reliability of a signature. Furthermore, *Article 7 of the MLES* provides that _any person, organ or body, whether public or private certified by the enacting state as competent, may determine which signature satisfies the provision of *Article 6*'[227]. It also provides that a determination of reliability as provided for in *Article 6* must be consistent with _International Standards'[228]. In addition, the Guide to the enactment of the MLES defines standards thus:

> the notion of "standard" should not be limited to official standards developed, for example, by the International Standards Organization (ISO) and the Internet Engineering Task Force (IETF), or to other technical standards. The word "standards" should be interpreted in a broad sense, which would include industry practices and trade usages, texts emanating from such international organizations as the International Chamber of Commerce… as well as the work of UNCITRAL itself (including these Rules and the Model Law). The possible lack of relevant standards should not prevent the competent persons or authorities from making the determination referred to in paragraph (1)…[229]

In terms of the MLES, it can be surmised that an electronic signature which satisfies the following requirements is valid:

(a) It is reliable as is appropriate for the purpose for which the data message was created or communicated;
(b) The signature creation data can only be attributed or ascribed to the signatory;

[225] Article 7 UNCITRAL MLEC.
[226] Article 6 (3) of UNCITRAL MLES.
[227] Article 7 (1) of UNCITRAL MLES.
[228] Article 7 (2) of UNCITRAL MLES.
[229] Guide to the UNCITRAL MLES, at para 135.

(c) Any alteration made to the electronic signature after the signature was affixed is detectable;
(d) The signatory was the only person in control of the signature creation data at the time of signing;
(e) Any alteration to any information whose integrity is required to be secured by a signature is detectable[230].

Essentially, all of these requirements are mandatory, for an electronic signature to be valid. Having completed a discourse on the Model Laws, a detailed exploration of other international Legal instruments regulating e-commerce is pertinent.

3.4 The Uniform Rules of Conduct for Interchange of Data by Teletransmission (UNCID).

The Uniform Rules of Conduct for Interchange of Data by Teletransmission (UNCID) are a set of voluntary guidelines published by the ICC[231], as far back as 1987, to facilitate the use of Electronic Data Interchange (EDI). The UNCID rules were aimed at facilitating the interchange of trade data through teletransmission, the creation of agreed rules of conduct between parties engaged in such transaction[232]. The UNCID rules are relevant to this paper due to the fact that it represents the oldest instrument created to regulate e-commerce. At this point, a cursory review of the concept of EDI is apposite, in order to facilitate an understanding of this regulation.

3.4.1 Electronic Data Interchange (EDI).

EDI is a form of Electronic Commerce which lends credence to the fact that the potential of conducting business using computer technology is not a novel idea introduced by the internet revolution[233]. EDI is reported to have been commonly used since the 1980s and is still in use till date[234]. The difference between EDI and the internet is that in the former, communications take place within a closed network, while in the latter, communication takes place over an open network[235]. Simply put, EDI is the computer-to-computer exchange of business documents in a

[230] Article 6 of UNCITRAL MLES.
[231] International Chamber of Commerce.
[232] United Nations Economic Commission for Europe website, accessed at http://www.unece.org/tradewelcome/areas-of-work/un-centre-for-trade-facilitation-and-e-business-uncefact/outputs/standards/unedifact/tradeedifactrules/part-2-uniform-rules-of-conduct-for-interchange-of-trade-data-by-teletransmission-uncid/part-2-uncid-chapter-4-interchange-agreement.html, on the 13th of May, 2014, at 05:05pm.
[233] C, Indira: International Trade Law, (2005), 3rd ed, Cavendish Publishing Limited, p.107.
[234] Ibid.
[235] Ibid.

standard format between business partners[236]. It denotes a significant shift from paper-based methods of dealing to electronic methods (which, in a nutshell sums up e-commerce). This technology enables value-chain partners to exchange purchase orders, advance ship notices, invoices, and other documents directly, from one computer system to the other, without human intervention[237].

In addition, EDI may also be used in tracking shipments, sending orders to warehouses and creating invoices[238]. For instance, it may serve as an invaluable tool to an e-commerce retailer, as it may be employed in the online sale of goods, for the transfer of order information to warehouses. The proven advantages[239] of EDI are: fewer data entry errors, greater efficiency, lower administrative costs, faster order to cash cycle.

The increased use of EDI technology significantly impacted on the nature of international trade, as the shift from paper-based transactions to electronic alternatives became pronounced, particularly in Europe, North America, Asia and Australia[240]. For instance, rather than sending and receiving original written documents with handwritten signatures, traders began to transfer structured business data from one computer system to another by electronic means including the increased use of electronic signatures[241]. This shift resulted in industries creating their own standards, for example, the motor industry in Europe created its own standard in ODETTE[242], while the chemical industry had CEFIC[243]. These standards usually stipulate the type of documents that can be transmitted electronically (for example an invoice), as well as the order, the sequence and the interpretation of the data[244].

---

[236] Edibasics website, _What is Edi?' accessed at http://www.edibasics.com/what-is-edi/, on the 13th of May, 2014, at 02:10pm.
[237] Accessed at http://www-01.ibm.com/software/commerce/b2b/edi/, on the 13th of May, 2014, at 02:28pm.
[238] Accessed at http://www.techterms.com/definition/edi, on the 13th of May, 2014, at 02:28pm.
[239] Accessed at http://www-01.ibm.com/software/commerce/b2b/edi/, and at http://www.highjump.com/solutions/truecommerce/what-is-edi , on the 13th of May, 2014, at 02:28pm.
[240] _An Introduction to Interchange Agreements', accessed at http://www.unece.org/tradewelcome/areas-of-work/un-centre-for-trade-facilitation-and-e-business-uncefact/outputs/standards/unedifact/tradeedifactrules/part-2-uniform-rules-of-conduct-for-interchange-of-trade-data-by-teletransmission-uncid/part-2-uncid-chapter-4-annex.html on the 13th May, 2014, at 07:14pm.
[241] Ibid.
[242] Organisation for Data Exchange by Teletransmission in Europe; www.odette.org.
[243] Counseil Europeen des Federations l'Industrie Chimique; www.cefic.be.
[244] Indira (note 233 above) 108.

However, the extent to which national and international legislations accepted the utility of electronic signatures as performing the same function as the handwritten signatures varied considerably; hence the need for unifying regulations in this regard. UNCID is therefore a response to the increasing commercial interest in the use of EDI.

3.4.2 Overview of the UNCID.

The UNCID rules are aimed at facilitating the interchange of trade data by Teletransmission (EDI) in International Trade[245]. It is important to note that the focus of this set of rules is the creation of an enabling environment for data interchange, and the content of such data falls outside the purview of this code of conduct[246]. The UNCID aims at ensuring that electronic data interchanges are secure, by stipulating that parties include certain measures to ensure authenticity of data messages, in their EDI transactions. For instance, while the sender is required to verify that each message is correct and complete before sending[247], the recipient is also required to acknowledge receipt, where the sender specifically stipulates this, and is precluded from acting upon the received message until such acknowledgement is forwarded to the sender[248]. In addition, the parties are required to include techniques for the verification of the relevant parties to their EDI transactions[249].

Furthermore, the recipient is required to confirm to the sender that the content of the data received appears to be correct in substance[250]. In addition, in the event that a party receives a message, which he is convinced was not intended for him, he must promptly delete it and inform the sender[251]. Moreover, the parties are expected to apply some measure of protection, by way of encryption, or some other means agreed upon, to all or some of the data messages

[245] Article 1, UNCID Rules, accessed at www.unece.org/index.php?id=24851, on the 13th May, 2014, at 12:23pm.
[246] Article 1 UNCID: ‗Article 1: Objective
These rules aim at facilitating the interchange of trade data effected by teletransmission, through the establishment of agreed rules of conduct between parties engaged in such transmission.
Except as otherwise provided in these rules, they do not apply to the substance of trade data transfers'.
[247] Article 6(a) UNCID.
[248] Article 7(a) UNCID.
[249] Article 6(b) UNCID.
[250] Article 8(a) UNCID.
[251] Article 7(d) UNCID.

exchanged via electronic interchange[252]. The UNCID mandates parties to maintain a data log of all sent and received data, in their actual state, without modification[253].

Despite the lofty ideals set out in the UNCID, it is essential to reiterate that the UNCID rules were specifically developed for closed networks, and it was inadequate to establish trust and reliability in open networks in which the internet operates. In addition, the UNCID rules, served as an open-ended guide, in the sense that it laid down certain rules to afford the security of transactions, but left parties to adopt particular methods they deemed suitable for their particular transactions.

Fundamentally, the increased popularity of the internet, and by extension, open network e-commerce transactions, served as an impetus for the ICC to undertake to publish international guidelines for e-commerce on the open network. This resulted in the issue of the General Usage for International Digitally Ensured Commerce (GUIDEC) in 1997, which would be discussed in a bit more detail below.

3.5 General Usage for International Digitally Ensured Commerce (GUIDEC).

The GUIDEC is a comprehensive statement of best practices to be adopted by business institutions and governments alike, in the use of e-commerce, for a uniform global infrastructure[254]. It is aimed at promoting confidence in the use of the e-commerce technology and was first published in 1997[255]. The prime objective of the GUIDEC is the establishment of a uniform framework for the authentication of digital messages, based on the existing law and practice in various legal systems[256]. It is essential to note that the GUIDEC is a general framework put forth by the ICC, based on the existing common law and civil law treatment of the subject of the use of techniques in electronic commerce, as well as pertinent international principles[257]. The GUIDEC was created as a living document, which means that it is open to

[252] Article 9(a) UNCID.
[253] Article 10(a) UNCID.
[254] Introduction to GUIDEC II, The International Chamber of Commerce website, accessed at http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2001/GUIDEC-General-Usage-for-International-Digitally-Ensured-Commerce-(Version-II)-01/10/2001/, on the 13th May, 2014 at 12:29pm.
[255] Indira (note 233 above) 117.
[256] Introduction to GUIDEC II, (note 254 above).
[257] Article 1, GUIDEC II, accessed at http://cryptome.org/jya/guidec2.htm, on the 17th, May, 2014 at 12:35pm.

modifications, as new technologies in e-commerce are developed[258]. In addition, it contains a glossary of core concepts and various best practice examples, which may be referred to, for clarification by bodies seeking to rely on its provisions[259].

A second version of these set of rules, titled GUIDEC II was published in 2001. The first version of the GUIDEC was directed at highlighting the key elements involved in the use of e-commerce, to serve as an indicator of the terms, while expounding on the general background to e-commerce[260]. It also addresses certain problems regarding e-commerce contracting, such as the use of electronic signatures[261]. Thus, the second version is basically an improvement on the previous version and expands on certain areas of relevance to businesses[262]. It is expanded to include the potential of additional technologies, such as biometrics in establishing security in digital transactions, while taking cognizance of related policy documents such as the UNCITRAL MLEC.

The GUIDEC defines the UNCITRAL MLEC as embodying the most definitive treatment of issues regarding international electronic commerce. It further states that the UNCITRAL MLEC however fails to address certain surrounding issues, which it therefore seeks to expand and build upon[263]. The GUIDEC defines requirements for signatures used in international commerce, particularly digital signatures, and it adds the requirement of certification[264]. It is pertinent to state that the GUIDEC is a useful instrument for the regulation of e-commerce, although it lacks wide application. It may be suggested that governments may look upon the texts of this instrument, in addition to the Model Laws, or as a supplementation of the principles which the Model Laws fail to cover, in order to develop a well-rounded e-commerce

[258] _General Usage for International Digitally Ensured Commerce' accessed at http://ecommerce.hostip.info/pages/477/General-Usage-International-Digitally-Ensured-Commerce-GUIDEC.html on the 16th of May, 2014 at 07:35pm. This is similar to the technological neutrality feature of the UNCITRAL Model Laws as discussed above.
[259] Ibid.
[260] Foreword to GUIDEC II, The International Chamber of Commerce website accessed at http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2001/GUIDEC-General-Usage-for-International-Digitally-Ensured-Commerce-(Version-II)-01/10/2001/, on 13 May, 2014 12:29pm, 3.
[261] Ibid 3.
[262] Introduction to GUIDEC II, The International Chamber of Commerce website, accessed at http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2001/GUIDEC-General-Usage-for-International-Digitally-Ensured-Commerce-(Version-II)-01/10/2001/, on 13 May, 2014 12:29pm.
[263] Ibid.
[264] Ibid 7.

framework. Having noted the operation of GUIDEC, it is necessary to review the European Union Directive on Electronic Commerce.

3.6 The European Union Directive on Electronic Commerce (Directive 2000/31/EC).

The Directive 2000/31/EC was adopted in the year 2000 and is commonly referred to as the e-commerce directive or the Directive on e-commerce[265]. It squarely deals with central issues pertaining to e-commerce such as commercial communication[266], formation of online contracts and the liability of intermediaries[267]. It is aimed at providing ‗Legal certainty for business and consumers alike', and seeks to achieve this aim by ‗establishing harmonised rules on issues such as transparency and information requirements for online service providers, commercial communications, electronic contracts and limitations of liability of intermediary service providers'[268].

This directive varies from the MLEC discussed above in that its focus is the free movement of ‗information society services' among its member states and the protection of the online consumer. Although it deals with a number of contractual matters; while the model law is a global framework, not circumscribed to any particular region, nor binding, but aimed at serving as a guide to legislators, in a bid to harmonizing the global legal framework regulating e-commerce contracting. The term ‗information society services' has been defined as any service for which remuneration is provided, at a distance, via electronic means and at the individual request of the recipient(s)[269].

The directive is set against the background of the life-cycle of e-commerce activities[270]. The reasoning is that a service provider first establishes a network connection, then, he

[265] A.R Lodder: ‗Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market', ch 4, accessed at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1009945, on the 9th of May, 2014, at 4:58pm.
[266] Commercial Communication is defined in Article 2 of the EU Directive as ‗any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession...'
[267] Lodder (note 265 above).
[268] ‗The EU Single Market', the European Commission website, accessed at http://ec.europa.eu/internal_market/e-commerce/directive/index_en.htm, on the 20th of May, 2014, at 09:13am.
[269] D.Sparas: ‗EU Regulatory Framework for e-commerce', presented at the WTO workshop in Geneva on the 18th June, 2013, accessed at http://www.wto.org/english/tratop_e/serv_e/wkshop_june13_e/sparas_e.pdf, on the 9th of May, 2014, at 4:55pm, 6.
[270] Lodder (note 265 above).

communicates commercially and then, concludes his contract[271]. However, during the course of contracting, the liability of intermediaries may arise and the need to resolve conflicts borne of this development arises. The objectives of the directive are based on the principles enshrined in _A European Initiative in Electronic Commerce', which provides that the first objective is to build trust and confidence of consumers and businesses in the legality as well as the security of e-commerce transactions[272]. While the second objective identified was to ensure full access for electronic commerce in a single market place[273]. The following are some of the objectives of the Directive[274]:

- Remove obstacles to cross-border online services in the EU internal market (free movement of information society services between member states)[275];
- Provide legal certainty to business and citizens[276];
- Offer a flexible, technically neutral and balanced legal framework[277]; and
- Enhancing competitiveness of European service providers.

3.6.1 Overview of Salient aspects of the EU Directive.

It can be deduced from the Directive that it covers a wide range of activities, such as the sale of goods, accountancy, medical and legal services offered via an open or closed communication

[271] For instance, by first setting up a website he establishes a network connection, then, by displaying his items for sale/ detailing the services he aims at rendering (as the case may be), he communicates commercially, and by engaging in an actual sale or the providing of a service, the contract is concluded (analogy mine). Lodder (note 265 above).
[272] COM (97) 157, 15.04.97 (at para 35-38), sourced from Indira, (note 233 above) 118.
[273] Which this thesis believes the EU Directive addresses. COM (97) 157, 15.04.97 (at para 35-38), sourced from Indira (note 233 above) 118.
[274] Sparas (note 269 above) 4.
[275] Article 4 of the EU Directive.
[276] Legal certainty is aimed at being achieved by having a specific set of e-commerce Laws for the European Union region, such that parties contracting within this region have a common governing regime(EU Directive) as regards salient aspects of their contracts, such as the signature requirements, time and place of dispatch requirements and so on. This makes for Legal certainty.
[277] This directive was introduced with the aim of harmonising and clarifying issues of online contracting throughout Eurrope and applies principles of technical neutrality and functional equivalence, as discussed above. This in turn ensures a flexible, technologically neutral and balanced Legal framework. The Directive applies to the member states of the European Economic Area (EEA), this includes the 27 member states of the EU plus Norway, Iceland and Liechtenstein. _The UK's E-Commerce Regulations' accessed at http://www.out-law.com/page-431, on the 9th May, 2014, at 4:53pm.

network, such as the internet[278]. Examples of services covered by the Directive include online information services (such as online newspapers), online selling of products and services (books, financial services and travel services), online advertising, professional services (lawyers, doctors, estate agents), entertainment services and basic intermediary services (access to the Internet and transmission and hosting of information)[279].

It however expressly provides that the following activities fall outside the scope of its application[280]:

- the activities of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority;
- the representation of a client and defence of his interests before the courts; and
- gambling activities which involve wagering a stake with monetary value in games of chance, including lotteries and betting transactions.

Article 4 of the EU Directive provides that ‗Member States shall ensure that the taking up and pursuit of the activity of an information society service provider may not be made subject to prior authorisation or any other requirement having equivalent effect'. This means that a broker, for instance, wishing to offer his insurance products over the internet needs not obtain prior authorization for doing so[281]. Although the information society service provider is required to meet certain transparency requirements as stipulated in the directive. The transparency provision operates to serve as an assurance to the consumer that the service provider has a traceable offline identity[282]. According to *Article 5* of the said Directive, an information society service provider is required to make the following information available in an easy, direct and in a permanently accessible manner, at the very least:

> (a) the name of the service provider;
>
> (b) the geographic address at which the service provider is established;
>
> (c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner;

[278] Indira (note 233 above) 119.
[279] These services include also services provided free of charge to the recipient and funded, for example, by advertising or sponsorship. ‗The EU Single Market', the European Commission website, accessed at http://ec.europa.eu/internal_market/e-commerce/directive/index_en.htm, on the 20th of May, 2014, at 09:13am.
[280] Article 1(5) (d) of the EU Directive.
[281] Indira (note 233 above), 119.
[282] Ibid, 119.

(d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register;

(e) where the activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority[283].

In the event that the service purported to be rendered is that of a regulated profession, additional information is required to be supplied, such as the registered professional body the service provider belongs[284]. These measures are set against the background of the underlying principles of the Directive, of imbuing consumers and businesses with trust and confidence in e-commerce, as alluded to above.

3.7 Conclusion.

The shift to an open communication network by the use of the internet poses a significant challenge to the global implementation of an electronic trading system[285]. One of the most significant barriers to global e-commerce pertains to the security of the information involved[286]. The implementation of security measures and mechanisms to reduce the risk of fraud as well as unauthorized access is crucial to the growth of the number and volume of international transactions over open networks. Appropriate information security is central to ensuring confidence and trustworthiness in open communication networks contracting, and e-commerce at large.

Conjunctive efforts have been made in a bid to ensure security in e-commerce transactions by members of industry and stake holders and have yielded in some of the policy documents discussed above. However, these are shades of self-regulation; which need to be complemented by Government Regulations for binding effect. Moreover, the extent to which these regulations can go in achieving this purpose is a well mooted subject.

[283] Article 5(1)(a)-(e) of the EU Directive.
[284] Article 5(1)(f) of the EU Directive.
[285] ‗An Introduction to Interchange Agreements', accessed at http://www.unece.org/tradewelcome/areas-of-work/un-centre-for-trade-facilitation-and-e-business-uncefact/outputs/standards/unedifact/tradeedifactrules/part-2-uniform-rules-of-conduct-for-interchange-of-trade-data-by-teletransmission-uncid/part-2-uncid-chapter-4-annex.html on the 13th May, 2014, at 07:14pm.
[286] Yee Fen Lim (note 136 above) 220.

A detailed analysis of how the provisions of the Model Laws can be relevant to African Countries would be undertaken in the next two chapters. However, chapter four would border on the Legal framework in the selected countries under review and the effectiveness of these Legal regimes would be analysed. Then, a further analysis of these Legal regimes would be undertaken in chapter five, by way of a comparative analysis.

CHAPTER FOUR: THE E-COMMERCE LEGAL FRAMEWORK IN SELECTED COUNTRIES.

4.1 Introduction: Challenges Facing African Countries.

The emergence of Information and Communication Technology (ICT[287]) has significantly impacted on the conduct of businesses across the globe[288]. Its impact cuts across the business sector to the entertainment sector, the banking sector and a host of other commercial sectors[289]. The ICT has remained the dominant platform for business activities[290] and various activities are being carried out electronically, due to the adoption of ICT. The platforms offered for commercial transactions include the internet, the web, mobile devices, all collectively regarded as e-commerce[291] through the use of e-mail and even e-government mechanisms[292]. Consequently, this has resulted in the increased efficiency of these sectors, while simultaneously reducing the barriers of time, distance and cost, which had previously characterized international trade[293].

Moreover, the advent of the ICT revolution has the potential of contributing substantially to poverty eradication in Africa, through the medium of e-commerce[294]. For instance, e-commerce

---

[287] ICT is an umbrella term which includes any communication device or application, encompassing radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing, distance learning and even online shopping. M, Rouse ‗Information and Communications Technology or Technologies', accessed at http://searchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies, on the 5th September, 2014 at 2:15pm.

[288] AO Oyewunmi: ―The ICT Revolution and Commercial Sectors in Nigeria: Impacts and Legal Interventions", British Journal of Arts and Social Sciences, vol. 5, No. 2 2012,ISSN 2046-9578, accessed at http://www.bjournal.co.uk/paper/bjass_5_2/bjass_05_02_08.pdf, on the 4th March, 2013 at 06:12pm, 234-248, at 235.

[289]Ibid.

[290] C. K. Ayo; A. A. Adebiyi; I.T. Fatudimu, and U. O. Ekong , ‗A Framework for e-Commerce Implementation: Nigeria a Case Study' (2008), Journal of Internet Banking and Commerce, August 2008, vol. 13, no.2, accessed at http://www.arraydev.com/commerce/jibc/2008-08/ayo.pdf, on the 6th September, 2014 at 5:28pm.

[291] Ibid.

[292] Guriting P, Ndubisi NO (2006). ―Borneo online banking: evaluating customer perceptions and behavioural intention" Manage. Res. News, 29(1/2) : 6-15

[293] Oyewunmi,(note 288 above) 235.

[294] For examples of the deployment of ICT mechanisms for the facilitation of agricultural development and entrepreneurship in Africa, M, Gakuru, K, Winters and F, Stepman, ‗Inventory and Innovative Farmer Advisory Services Using ICTs', is instructive, being an initiative of the Forum for Agricultural Research in Africa, 2009, last accessed at http://www.fara-africa.org/media/uploads/File/NSF2/RAILS/Innovative_Farmer_Advisory_Systems.pdf , on the 5th September 2014 at 2:38pm.

creates an avenue for the promotion of local products in the international market[295], while the ICT mechanism arms an entrepreneur with relevant market information to set competitive prices while aiding the effective functioning of the market. On the other hand, the new technology has heralded new horizons of crime, generally regarded as cyber-crime or internet crime, by persons who have chosen to direct the technology to achieving dubious or fraudulent ends[296]. Examples of cyber-crimes include: child pornography, fraudulent electronic funds transfers, unauthorized access to computer systems and so on[297]. This presents numerous challenges to African Countries as well as several other countries across the globe.

The crux of the discussions in this chapter revolves around the peculiar challenges which African countries are faced with, in terms of e-commerce. Some of these challenges range from poverty, underdevelopment and lack of accurate internet penetration. This has resulted in a large proportion of the people in the continent being unable to benefit from the e-commerce industry, both from the consumer and merchant blocs. In assessing the situation, Afaedor, an expert in the e-commerce industry in Nigeria, highlighted some basic factors, which he qualified as obstacles to the growth of e-commerce in Nigeria.

According to him, lack of basic infrastructure like steady power supply, available technological expertise, funding for entrepreneurs, good roads as well as limited access to telecommunication infrastructure and high cost of Internet, could hinder the growth of e-commerce in Nigeria[298]. Furthermore, he opined that although Nigeria's e-commerce had grown steadily, the lack of legislation that specifically targets cyber-crime or cyber security had no doubt continually hampered its accelerated growth[299]. Moreover, the concerns raised by such nefarious activities, no doubt, calls for legal intervention.

---

[295] Evidence of this can be seen in websites such as - http://www.alibaba.com/countrysearch/NG/craft-supplier.html, last accessed on the 5th September 2014 at 2:30pm.
[296] Oyewunmi, (note 288 above) 235.
[297] Ibid.
[298] 'E-commerce as the Next Driver for Nigeria's Economic Growth', Thisday Live online newspaper issue of the 28th February, 2013, accessed at http://www.thisdaylive.com/articles/e-commerce-as-next-driver-of-nigeria-s-economic-growth/140811/ on the 18th June, 2014, at 02:39pm.
[299] Ibid.

Recent studies have shown that people are more likely to engage in offensive or illegal behavior online because of the perception of anonymity, thus cyber criminals exploit the rights and privileges of a free society, including anonymity[300].

However, in South Africa, despite the fact that online shopping is not a novel concept in the region, a key problem encountered in its application is the dire need to educate consumers as regards this platform[301]. Furthermore, the country's large land mass, poor transport logistics, lack of broadband penetration, and a persistent lack of trust in online payments, are the highlighted factors which all hinder the expansion of online shopping, and by extension, e-commerce[302].

This chapter explores the existing legal regime regulating e-commerce in South Africa, analyses its implementation of this regime, in the light of decided cases. In addition, the situation in Nigeria is scrutinized, in the absence of a specific Legal instrument regulating e-commerce. Thereafter, the situation in the United Kingdom is evaluated, in the light of its Computer Misuse Act, to consider the impact of this legislation in addressing the challenges of e-commerce. A conclusion is thereby reached against the background of these studies.

4.2 South Africa.

4.2.1 Introduction.

Across the globe, various organisations have created websites for business and information purposes[303]. While some of these websites basically provide information, others provide some sort of interactivity with customers[304]. What is certain is that e-commerce is steadily gaining momentum across the globe. It is therefore against this background that firms are struggling to catch up with the thrust of the e-commerce wave.

---

[300] Ibid.
[301] Head of marketing at Interactive Advertising Bureau South Africa (IAB), Sarah Rice .R, Mahlaka ―Oline Shopping: Is SA ready for it?" Moneyweb online article accessed at http://www.moneyweb.co.za/moneyweb-south-africa/online-shopping-is-sa-ready-for-it, on the 17th June, 2014 at 04:58pm.
[302] Ibid.
[303] R, Dagada, MM Eloff, & LM Venter _Too Many Laws but very Little Progress! Is South African Highly Acclaimed Information Security Legislation Redundant', (2009) 3, accessed at http://icsa.cs.up.ac.za/issa/2009/Proceedings/Full/4_Paper.pdf, 18 July, 2013 at 11:04am.
[304] Ibid, 3.

E-commerce in South Africa is reported to have experienced a tremendous growth in the past two decades[305], fuelled by the realization that online procurement and supply chain management play the dual function of cutting back costs and improving customer relationships[306]. Accordingly, a number of large South African firms, such as those in the mining, chemical, manufacturing and financial services sectors, conduct their businesses employing ICT mechanisms, especially e-commerce, in line with global standards[307].

The Electronic Communications and Transactions Act[308] is South Africa's primary legislation regulating e-commerce activities in the Republic. Prior to the promulgation of the ECTA, e-commerce was regulated by South Africa's Common Law and Statutory Law[309]. The inadequacy of South Africa's Common law to effectively address problems emanating from e-commerce transactions prompted the promulgation of this substantive legislation[310]. In the wake of this realisation, the South African Government set out to develop a legal framework to foster security, transparency and infrastructural commercial development[311]; hence, the birth of the ECTA. It is apposite to state that the ECTA is a fused prototype of the UNCITRAL MLEC[312] and the UNCITRAL MLES[313].

[305] ZN Jobodwana _E-Commerce and Mobile Commerce in South Africa: Regulatory challenges' (2009) Journal of International Commercial Law and Technology, 4.
[306] Ibid, 4.
[307] Ibid, 4.
[308] 25 of 2002, hereafter referred to as ECTA.
[309] F, Cassim, _Formulating Specific Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study' P.E.R, vol. 12, no. 4, 2009, accessed at http://www.nwu.ac.za/files/images/2009x12x4_Cassim_art.pdf on the 14th January, 2014, at 06:34pm, 36-79, 55.
<http://www.puk.ac.za/opencms/export/PUK/html/fakulteite/regte/per/issuepages/2009Volume12no4/2009x12x4_Cassim_art.pdf>, accessed 14th January, 2014, 6:50pm.
[310] D, Goodburn, & M, Ngoye: _Privacy and the Internet' (In: R Buys & F Cronje, Cyberlaw: The Law of the Internet in South Africa, Van Schaik Publishers, 1 ed. (2004) 97-112) in Dagada, Eloff & Venter (note 303 above), 6.
[311] J, Hofman, , D, Johnston, S, Handa & C, Morgan, C, Cyberlaw: A Guide for South Africans Doing Business Online, Cape Town: Ampersand. Dunlop (2005), in Dagada, Eloff & Venter (note 303 above), 6.
[312] The United Nations' Commission of International Trade Law (UNCITRAL) Model Law on Electronic Commerce (MLEC).
[313] The United Nations' Commission of International Trade Law (UNCITRAL) Model Law on Electronic Signatures (MLES).

4.2.2 Overview of Salient aspects of the Electronic Communications and Transactions Act.

The aims of the act are:

> to provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy for the Republic; to promote universal access to electronic communications and transactions and the use of electronic transactions by SMMEs; to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of e-government services; and to provide for matters connected therewith[314].

Essentially, *Section 3,* which embodies the interpretation clause of the Act, accommodates the applicability of Common law or other Statutory Law, which recognizes electronic transactions to the effect that in the event that the ECTA does not provide specific regulations as regards certain matters or offence, such common or statutory law applies.

Chapter III of the Act deals with the facilitation of Electronic Transactions. Part 1 of Chapter III addresses the Legal Requirements for Data Messages[315], such as the requirements of writing, signature, original and evidential weight to be attached.

Section 11 imparts the legal recognition of a data message by prohibiting the discrimination against a data message by virtue of its form. It lays the foundation for the admissibility of data messages, thus: ‗Information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message'[316].

Further, *Section 11* provides that:

> ‗Information is not without legal force and effect merely on the grounds that it is not contained in the data message purporting to give rise to such legal force and effect, but is merely referred to in such data message'[317]

As regards the legal requirement of writing in e-commerce, *Section 12* provides to the effect that this requirement is met by a data message if the information contained in the data message is capable of being accessed subsequently. It provides:

---

[314] Preamble to the Electronic Communications and Transactions Act.

[315] This refers data generated, sent, received or stored by electronic means, and includes voice, where such voice is used in an automated transaction and a stored record- *Section 1 ECTA.*

[316] *Section 11 (1) ECTA.*

[317] In essence, it bars the denial of legal force and effect given to information referred to in a data message on the basis that it is not contained in such data message, but merely referred to. *Section 11 (2) ECTA.*

> A requirement in law that a document or information must be in writing is met if the document or information is in the form of a data message and accessible in a manner usable for subsequent reference'[318].

In terms of the legal requirement of signatures, the Act outlaws the denial of validity of an electronic signature solely on the grounds of its form[319]. Furthermore, *Section 13* of the Act provides that:

> Where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature is used'[320].

In addition, the act aims at imparting a measure of security and reliability in e-commerce transactions amongst parties. This is achieved by setting out the twin tests for the validity of an electronic signature, while giving parties the reins to decide on the particular technology to employ[321]. The first is the capability of the electronic signature of identifying a party and indicating such party's approval of communicated information[322]. While the second is the reliability and appropriateness of the technology employed, in relation to the purpose for which the information was created[323].

Section 13 further provides:

> Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if
>
> (a) a method is used to identify the person and to indicate the person's approval of the information communicated; and
>
> (b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated[324].

[318] *Section 12 (a) & (b) ECTA.*
[319] *Section 13 (2) ECTA.*
[320] *Section 13 (1) ECTA.*
[321] *Section 13 (3) ECTA.*
[322] *Section 13 (3) (a) ECTA.*
[323] *Section 13 (3) (b) ECTA.*
[324] *Section 13 (3) ECTA.*

Moreover, the requirement of originality by a data message is covered by *Section 14*. It states that the requirement that information be presented in its original form is met in relation to a data message if:

- the integrity of the information has remained intact from the time of its generation in its final form, in the light of the purpose for its generation and other relevant circumstances[325]; and
- The information is capable of being displayed to whosoever it is being presented[326].

It provides:

> (1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if -
>
> (a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and
>
> (b) that information is capable of being displayed or produced to the person to whom it is to be presented.
>
> (2) For the purposes of subsection 1 (a), the integrity must be assessed-
>
> (a) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;
>
> (b) in the light of the purpose for which the information was generated; and
>
> (c) having regard to all other relevant circumstances.

Additionally, the issue of admissibility and evidential weight of data messages are addressed in *Section 15*. *Section 15(1)* sets out the non-discrimination (a feature of the model Law) against data messages by virtue of their form. It states that data messages should not be denied admissibility in evidence solely on the grounds that it is a data message[327] or that it is not in its original form[328]. It provides further, that-

> in assessing evidential weight of a data message, regard shall be had to:
> a) the reliability of the manner in which the data message was generated, stored or communicated;
> b) the reliability of the manner in which the information was maintained;

[325] The combined effect of *Section 14 (1) & (2) ECTA.*
[326] *Section 14 (1) (b) ECTA.*
[327] *Section 15 (1) (a) ECTA.*
[328] *Section 15 (1) (b) ECTA*

c) the manner in which the originator was identified; and
d) any other relevant factor[329].

Chapter XIII[330] addresses the issue of cyber-crime, while *Section 86* therein, outlaws the unauthorized access to, interception of and interference with data, *Section 87* criminalises Computer related extortion, fraud and forgery. Certain offences peculiar to e-commerce have been addressed by the ECTA. For instance, anti-hacking laws, which prohibit the design, production or sale of any security circumventing technology are made, by virtue of the combined effect of *Section 86(3) and Section 86(4)*. E-mail bombing and spamming are addressed in *Section 86(5) and Section 45* accordingly. Any person who commits any of the highlighted acts, or aids and/or abets their commission is guilty of an offence[331]. Interestingly, the penalties are liability ‗to a fine or imprisonment for a period not exceeding 12 months'[332] and liability ‗to a fine or imprisonment for a period not exceeding 5 years'[333] respectively.

Ancillary to the issue of cyber-crime is the creation of the office of cyber inspectors, which is set out in chapter XII[334]. A cyber inspector is empowered to ‗monitor and inspect any web site or activity on an information system in the public domain, and report any unlawful activity to the appropriate authority'[335]. In line with his powers of inspection alluded to, a cyber-inspector is authorized to perform such other functions supplementary to the performance of his roles. This includes the searching of any premises or information systems which has a bearing on an investigation, without prior notice, while armed with a warrant to do so[336].

Furthermore, the issue of jurisdiction is addressed by the ECTA in *Section 90*, it provides:

> A court in the Republic trying an offence in terms of this Act has jurisdiction where -
>
> (a) the offence was committed in the Republic;

[329] *Section 15 (3) (a) – (d) ECTA.*
[330] Spans from *Section 85-89 ECTA.*
[331] *Section 88(1) & (2) ECTA.*
[332] *Section 89(1) ECTA.*
[333] *Section 89(2) ECTA.*
[334] Comprising of *Sections 80-84 ECTA.*
[335] *Section 81(1) (a) ECTA.*
[336] *Section 82(1) ECTA.*

(b) any act of preparation towards the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic;

(c) the offence was committed by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic; or

(d) the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed[337].

Section 90 (a) reiterates the position prior to the implementation of ECTA, which is to the effect that South African courts, exercise jurisdiction over offences committed in the republic only[338]. While *Section 90 (b)* seems to widen the previously narrow instances where a South African court may exercise jurisdiction to include situations whereby preparations towards an offence or part of the offence took place in the republic or where the offence had an effect on the republic. The import of this section is that it addresses internet related crimes which are often perpetrated in one region, while resulting in catastrophic effects on another region, which previous legislation failed to address. For instance, where a virus is disseminated abroad, and wreaks havoc on computer networks in South Africa or when overseas based hackers hack into and damage South African computer systems, South African Courts are hereby vested with authority, by way of jurisdiction to pursue such perpetrators, due to the _effect' of these activities in the republic.

Likewise, South African courts are empowered with jurisdiction to try matters involving the commission of an offence by South African citizens, South African permanent resident holders and persons conducting business in the republic, irrespective of the location of the commission of the offence[339].

4.2.3 Implementation.

In terms of the implementation of the ECTA, there are a number of matters to be addressed. Firstly, the ECTA empowers cyber inspectors to enter any premises and access information which may impact upon an investigation into cyber-crime in *Section 82*. However, this

[337] *Section 90 (a) – (d) ECTA.*
[338] Although the exceptions to this rule include high treason, theft in a foreign country and offences committed on board ships or in aircrafts. Cassim, (note 309 above) 59.
[339] *Section 90 (c) ECTA.*

provision has been argued to be likely to operate as an infringement on the right to privacy provision of *Section 14 of the Constitution of the Republic of South Africa, 1996*[340]. Furthermore, the Criminal sanctions imposed by the ECTA have been criticized for not being severe enough to warrant the deterrence from cyber-crimes[341]. In contrast, the *Regulation of Interception of Communications and Provision of Communications-Related Information Act*[342] (RICA) prescribes much stringent penalties[343].

Secondly, the jurisdictional provisions of the ECTA may be somewhat problematic to implement. As alluded to above, the ECTA empowers South African courts with jurisdiction to entertain matters involving perpetrators who may be abroad, but whose activities had an effect in the republic[344]; or matters involving South African citizens[345] or matters pertaining to offences committed on board a ship or aircraft registered in the republic[346], in addition to offences actually committed in the republic[347].

It is submitted that despite the fact that these provisions denote a positively progressive trend; the ECTA has sidestepped certain salient points. For instance, the provisions of *Section 90 (b) - (d) of the ECTA* differ significantly from the provision of Section *28 (1) (d) of the Magistrate Court Act*[348], which requires ‗the whole cause of action' to take place within a particular court or district, for the determination of jurisdiction. In the light of this, if the provisions of the ECTA conferring jurisdiction on South African Courts in terms of offences committed abroad, are to be implemented, the question arises as to which regional or district court has jurisdiction

[340]Cassim, (note 309 above) 59. *Section 14* provides that ―everyone has a right to privacy, which includes the right not to have- (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed".
[341]Ibid 59.
[342] *70 of 2002 (the RICA).*
[343] For instance, Section 51 of the RICA prescribes fines not exceeding R 2 000 000 or imprisonment not exceeding ten years. For juristic persons, fines may increase to a maximum of R 5 000 000. When contrasted with the maximum term of 5years stipulated by the ECTA, the ECTA stipulations seem somewhat trivial. This issue would be discussed in greater detail in paragraph 4.2.4.3 below.
[344] *Section 90 (b) ECTA.*
[345] *Section 90 (c) ECTA.*
[346] *Section 90 (d) ECTA.*
[347] *Section 90 (a) ECTA.*
[348] 32 of 1944. *Section 28(d)* provides: ―Saving any other jurisdiction assigned to a court by this Act or by any other law, the persons in respect of whom the court shall… have jurisdiction shall be the following and no other:… (d)any person, whether or not he or she resides, carries on business or is employed within the district or regional division, if the cause of action arose wholly within the district or regional division".

to hear the matter. At this point, it is apposite to take a cursory look at South African Courts' approach to the implementation of the provisions of the ECTA.

4.2.4 Case Law Pertaining to E-commerce in South Africa.

4.2.4.1 Narlis v. South African Bank of Athens[349].

This case was decided prior to the implementation of the ECTA, it is of interest to this discourse as it is one of the cases which served as an impetus to the eventual implementation of the ECTA. Here, the court decided that *Section 34 of the Civil Proceedings Evidence Act*[350]did not contemplate the admissibility of a computer print-out in evidence. The section provided for specific instances whereby statements made by a person may be admissible. The court held that a computer cannot be regarded as a person, hence, inadmissible. At this point it was obvious that the law regarding electronic data in legal proceedings required urgent redress[351].

4.2.4.2 S v. Ndiki[352].

This case also dealt with the admissibility of computer-generated evidence, but prior to the implementation of the ECTA[353]. Of utmost interest to this discourse is one of Van Zyl J's comments on the proper approach for the courts, which goes thus:

> It seems that it is often too readily assumed that, because the computer and the technology it represents is a relatively recent invention and subject to continuous development, the law of evidence is incapable or inadequate to allow for evidence associated with this technology to be admissible in legal proceedings. A preferable point of departure in my view is to rather closely examine the evidence in issue and to determine what kind of evidence it is that one is dealing with and what the requirements for its admissibility are[354].

The tenor of this statement is to the effect that the preferred method of dealing with computer-generated evidence and new technology generally, is an objective one, rather than a subjective one. Furthermore, courts are hereby encouraged to take the cautious approach of closely examining the evidence presented before them and attempting at determining the conditions for their admissibility, rather than dismissing them altogether, on account of their form. This

---

[349] 1976 (2) SA 573 (A).
[350] 25 of 1965.
[351] S.L, Snail, _Cybercrime in South Africa and African Perspectives', accessed at http://www.snailattorneys.com/cyber%20crime%20in%20South%20Africa%20and%20african%20perspectives.pdf, on the 11th July, 2014, at 10:36am, 13.
[352] 2008 (2) SACR 252; [2007] 2 All SA 185 (Ck).
[353] Snail (note 351 above) 11.
[354] 2008 (2) SACR 252, 53(d) – (e).

reasoning is interesting as it resonates the ethos of the current ECTA, hence it is of interest to this discourse[355].

4.2.4.3 R v. Douvenga[356].

In the instant case, the Court had to decide whether an accused employee GM Douvenga of Rentmeester Assurance Limited (Rentmeester) was guilty of a contravention of *Section 86(1)* (read with *Sections 1, 51 and 85*) of the ECTA[357]. It was alleged in this case that the accused, on or about 21 January 2003, in or near Pretoria, and in the district of the Northern Transvaal, intentionally and without permission to do so, gained entry to data which she knew contained confidential databases and/or contravened the provision by attempting to send this data containing her company's entire client database of over 30,000 names and addresses via e-mail to her fiancée to keep[358]. The accused intended to take the data with her to her new employment at an opposition company[359].

The accused was found guilty of contravening *Section 86 (1)* of the ECTA and sentenced to a R1 000 fine or imprisonment for a period of three months[360]. Opinions have been expressed in terms of the disproportionate nature of this sentence in comparison to the quantum of damage which could have been suffered by Rentmeester if the accused was successful at this attempt[361]. These views have been concisely captured in the phrase: _the worrying trend of passing out light sentences for computer-related crimes, with fines vastly out of proportion in comparison to the losses, or in this case, potential losses that could be borne by the victims' requires redress.[362]

---

[355] Section 15 ECTA.
[356] District Court of the Northern Transvaal Regional Division, Pretoria, case no 111/150/2003, 19 August 2003 (unreported).
[357] See Appendix A below, for the specific provision of the ECTA.
[358] SS Snail _Cyber Crime in South Africa- Hacking, Cracking and Other Unlawful Activities', (2009) 1 *JILT*, 1-13, 6, accessed at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/snail/, 16 July, 2014, 10: 19am.
[359] Ibid.
[360] Ibid.
[361] Electronic Law Consultancy article, 2005. Accessed at http://elc.co.za/article.php?subaction=showfull&id=1070363190&archive=&start_from=&ucat=1&, on the 16th July, 2014 at 11:12am.
[362] Ibid.

4.2.4.4 Ndlovu v. Minister of Correctional Services[363].

In terms of South Africa's law of evidence, a computer print-out falls under documentary evidence, and documentary evidence is ordinarily required to pass three hurdles for it to be admissible[364]. These include: the original version rule; the authenticity rule; and the hearsay rule[365]. Once a document passes these three tests, then it becomes admissible and the court deduces its evidential value, against the background of the required burden of proof. However, these tests are specially designed for paper documents, rather than electronic data messages, such as computer print-outs, which they are not well suited for[366]. Hence, the need for clarification in terms of data messages. In terms of the first test, *Section 15 (1) (b) of the ECTA* provides a succinct position to the effect that a data message is admissible if it is the best evidence the producer is reasonably expected to adduce and should not be denied admissibility on grounds of its failure to comply with the originality rule[367].

In the instant case, the minister relied upon a two-page computer print-out obtained from the computer system of the Department of Correctional Services, in making out a case against Ndlovu[368]. The court set out to determine whether a computer print-out, which happened to be a copy, complied with the best evidence rule or had to be properly proved before it could be admitted in evidence[369]. Moreover, the computer print-out had been extensively referred to by witnesses during the examination-in-chief and cross-examination stages of the trial[370]. The plaintiff raised an objection to its admissibility at the argument stage on the grounds that it was not an original document (thus, fails to satisfy the best evidence rule) and that it should be properly proved before being admitted by the court[371]. With regard to the objection, the court found that the plaintiff's failure to object to the admissibility of the computer print-out during the trial precluded the plaintiff from seeking to rely on the best evidence rule only during the argument. Furthermore, the court found that the plaintiff's extensive referral to the computer print-out prior to his objection, during the course of the trial amounted to a tacit waiver of the

[363] 2006 (4) All SA 165 (W).
[364] D, Collier, –Evidently not so Simple producing Computer Print-outs in Court", Juta's Business Law, Vol. 13 (1), ISSN 1021-7061, 6-9, 6.
[365] Ibid 6.
[366] Ibid 6.
[367] See Appendix A below, for the specific provision of the ECTA.
[368] Cassim (note 309 above) 61.
[369] Ibid, 61.
[370] Ibid, 61.
[371] Ibid, 61.

best evidence rule by the plaintiff[372]. In addition, on account of the fact that the document in question was generated by a computer, the court found the ECT to be applicable[373].

Against this background, the court analysed the admissibility of the computer print-out in terms of the provision of *Section 15 of the ECTA and Section 3 of the Law of Evidence Amendment Act*[374]. However, the court found the document admissible, not in terms of *Section 15 of the ECTA*, but rather, in terms of *Section 3 of the Law of Evidence Amendment Act*. This decision has been criticized for not providing clarity on the impact of *Section 15 of the ECTA* on the authentication rule and the hearsay rule; as well as the evidential weight to be attached to electronic evidence[375].

4.2.4.5 Jafta v. Ezemvelo KZN Wildlife[376].

The summary of the facts of the case are as follows: Jafta was offered a job at Ezemvelo KZN Wildlife, for the position of General Manager: Human Resources. An offer to this effect was sent to him via e-mail with the condition that his failure to respond would lead to the position being offered to another person, which he purports to have responded to. The same offer was made to him via a text message which he also claims to have responded to, and referred to his acceptance via e-mail. The human resources office claimed not to have received the email, but received the text message, in which she did not recall reading an affirmative response in, before she deleted it. Against this background, Ezemvelo appointed another candidate for the position while Jafta contends that he accepted the offer and instituted this action against Ezemvelo to claim damages for losses suffered as a result of Ezemvelo‘s breach of contract.

The court set out to determine whether Jafta‘s acceptances to the offer were valid in terms of the Common Law and whether the Ezemvelo could be deemed to have received the acceptances in terms of the ECTA[377]. The court found that Jafta‘s acceptance met the common law stipulations of a clear, unambiguous and unequivocal offer; acceptance corresponding with the offer and acceptance being made in the mode prescribed by the offeror. Although the court found that Jafta‘s e-mail was not received by Ezemvelo, as it did not enter its information

[372] Ibid 61.
[373] Collier, (note 364 above) 9.
[374] 45 of 1988.
[375] Collier, (note 364 above) 9.
[376] 2008 10 BLLR 954 (LC).
[377] P, Stoop, ‗SMS and E-mail Contracts: Jafta v. Ezemvelo KZN Wildlife‘, 21 *SA Merc LJ* (2009) 110–125, 111.

system as contemplated by the ECTA, nor was it capable of being retrieved. However, it was found to have received his SMS, based on which a contract of employment had come into existence. Ezemvelo's denial of acceptance of the SMS and failure to act upon it, was found to constitute a repudiation, which was unlawful, and for which Jafta was entitled to damages[378].

4.3 Nigeria.

4.3.1 Introduction.

The Federal Republic of Nigeria operates a Federal Constitutional Republic System of Government and is a former British colony, which gained independence on the 1st of October, 1960. It comprises of 36 states[379] and a Federal Capital Territory- Abuja[380]. It is located in West Africa and shares borders with the Republic of Benin, Niger, Cameroon and Chad[381]. It is often regarded as the 'giant of Africa' on account of its large population and economy[382]. It is the most populous country in Africa[383] and is quite popular for a number of factors. Of relevance to the instant discourse is the well-known '419 Scam[384]' phenomenon, named after the section of Nigeria's Criminal code which outlaws this criminal activity, and will be discussed shortly.

In respect of e-commerce legislation, it is rather unfortunate to note that Nigeria is yet to implement a legal framework facilitating e-commerce, despite being the country with the highest number of internet users in the Continent[385]. There is currently a Legislative Bill before the Nigerian Legislature titled: 'the Bill for an Act to Provide for the Prohibition, Prevention, Detection, Response and Prosecution of Cyber Crimes and Other Related Matters 2013' which has been passed into Law by the Senate, but is yet to receive Presidential assent. Pending the operation of this Bill, the judiciary is left to decide upon matters arising from Electronic

[378] Ibid.
[379] Section 3(1) of the 1999 Constitution of the Federal Republic of Nigeria. See Appendix D below, for the specific provision of the Constitution.
[380] Section 3(4) of the 1999 Constitution of the Federal Republic of Nigeria. See Appendix D below, for the specific provision of the Constitution.
[381] Accessed at http://www.infoplease.com/country/nigeria.html, on the 5th of September, 2014 at 5:15pm.
[382] P, Holmes, 'Nigeria: Giant of Africa', 1987, National Oil and Chemical Marketing Company of Nigeria, 5.
[383] Accessed at http://www.infoplease.com/country/nigeria.html, on the 5th of September, 2014 at 5:15pm
[384] Nigeria-the 419 Coalition website, accessed at http://home.rica.net/alphae/419coal/, on the 5th of September, 2014 at 8:10pm.
[385] N. Ewelukwa, 'Is Africa Ready for Electronic Commerce? A Critical Appraisal of the Legal Framework for ECommerce in Africa'< http://www.acicol.com/temp/Dr N.pdf >, 18.

Commerce by resorting to several existing statutes, such as: The Statute of Frauds[386], the Evidence (Amendment) Act[387]; Advance Fee Fraud and other Fraud Related Offences Act 2006, and so on. At this point it is pertinent to explore the salient provisions of these Legislations.

4.3.2 The Laws.

The current *Evidence (Amendment) Act* contains the rules for the admissibility of electronically generated Evidence in Nigeria[388]. The situation prior to the promulgation of this amendment was characterized by confusion[389], as the Act dates as far back as 1945 and had amazingly survived time with little or no alterations, despite the radical 21st century technological advancements[390]. Essentially, the Nigerian courts were equally caught in the web of this confusion as well. In *Esso West Africa Inc. v. T. Oyegbola*[391], the Supreme Court of Nigeria held:

> _The law cannot be and is not ignorant of modern business methods and must not shut its eyes to the mysteries of the computer. In modern times reproduction or inscription on ledgers or other documents by mechanical process are common place and section 37 cannot therefore only apply to _books of account' so bound and the pages not easily replaced'.

[386] 1677, which forms part of Nigeria's received English Laws.
[387] Act No. 18 of 2011.
[388] E.U, Emuveyan: _Admissibility of Electronically Generated Evidence in Nigeria', LL.B Law Thesis, University of Lagos, Nigeria, July, 2013, 2. Accessed at <http://www.academia.edu/4186714/i_ADMISSIBILITY_OF_ELECTRONICALLY_GENERATED_EVIDENCE_IN_NIGERIADR_ABIODUN_ODUSOTE_DATE_SIGNATURE_PROJECT_SUPERVISOR_.._._.....PROF_TAIWO_OSIPITAN_DATE_SIGNATURETABLE_OF_CONTENTS> on the 23rd of July, 2014 at 3:18pm.
[389] Ibid.
[390] J.D Odi, _Admissibility of Electronic Evidence in Nigeria',2. The Nigerian Law of Evidence is substantially part of the received laws of Nigeria via section 45 of the Miscellaneous Provision Act of 1945(3). The Evidence Ordinance was passed as Ordinance No.27 of 1943. It did not take effect till the 1st of June, 1945 by virtue of Number 618 of Gazette Number 33 of 1945. Since the 1st of June, 1945, the Evidence Act has consistently retained its character 1951, 1960,1963,1976,1990 amendments notwithstanding. Subsequently, it was referred to as the Evidence Act Cap 112, 1990, Laws of the Federation. The Evidence Act remains the reference point on the law of evidence in Nigeria. However, section 5 of the Evidence Acts provides for the reception of evidence not specifically provided for by the act. Amazingly, the most recent amendment to the Evidence Act, titled *'the Evidence (Amendment) Act 2011'* is the focus of this paper, as it introduces notable amendments. See *The Challenges of Electronically Generated Evidence* Paper delivered by Hon. Justice Ohimai Ovbiagele LLB(HONS),BL,LLM,MPHILL,MBA,MA in Edo State, Nigeria. Accessed at <http://www.nigerianlawguru.com/articles/practice%20and%20procedure/THE%20CHALLENGES%20OF%20ELECTRONICALL%20GENERATED%20EVIDENCE.pdf>, on the 23rd of July, 2014, at 2:59pm.
[391] [1969] 1 N.M.L.R. 194 at 198; *YESUFU V ACB* (1976)4 SC 1.

In the words of Pats-Acholonu, JCA (Judge of the Court of Appeal) in *Egbue v. Araka*[392]:

> It must be clearly understood that our Evidence Act is now more than 50 years old and is completely out of touch and out of tune with the realities of the present scientific and technological achievements. Most of its sections are archaic and, anachronistic and needs a thorough overhaul to meet with the needs of our times. But alas, it is with us now like an albatross on our neck…

Regrettably, this was the situation, until the Amendment of the Evidence Act in 2011. It has been suggested that the greatest obstacle to the admissibility of electronic evidence under the old Evidence Act was its definition of ‗document', in terms of its restriction of this term to paper-based materials expressed in words and figures[393].

A Document is defined in *Section 258 of the Evidence (Amendment) Act*[394], to include

> ‗books, maps, plans, graphs, drawings, photographs, and also includes any matter expressed or described upon any substance by means of letters, figures or marks or by more than one of these means, intended to be used or which may be used for the purpose of recording that matter…'

A document is further defined to encompass:

> ‗any device by means of which information is recorded, stored or retrievable including computer output'[395]

This provision can clearly be extended to include electronic documents. It can be surmised that the purpose of this Legislation is to establish a recognition for non-paper based material, in line with current international trends, in the light of the current internet age. However, specific Legislation imparting Legal recognition to electronic documents is required, as this definition alone does not eliminate the obstacle to electronic documents' admissibility. For instance, Nigerian Law requires certain transactions to be evidenced in writing and signed. Such as: Hire Purchase Agreements, Marine Insurance Policies, Arbitration Agreements, and so on.

---

[392] [1996] 2 NWLR (Pt. 433) 688 C.A. at 710, para. A; 711 paras. C-G.
[393] E, Ikeh, ‗Towards a Legal Framework for the Development of E-Commerce in Nigeria: Issues and Prospects' February 2014, accessed at http://www.mondaq.com/x/294344/Contract+Law/Towards+A+Legal+Framework+For+The+Development+Of+ECommerce+In, on the 6th of September, 2014 at 5:28pm.
[394] Act No. 18 of 2011. Definition of document (a).
[395] Section 258, Definition of document (b).

While, *Section 4 of the Statute of Fraud, 1677* states that proceedings to enforce a contract for sale of land can only be brought where the contract or some memorandum or note of it, is in writing and signed by the person against whom the action is brought or that person's authorized agent[396]. Furthermore, the Nigerian courts have also held in a number of cases that ‗an unsigned document is a worthless document'[397]; in essence, electronic commerce presents some peculiarities in this regard[398].

In addition, *Section 18(1) of the Interpretation Act*[399] defines writing and expressions referring to writing to ‗include printing, lithography, photography, typewriting and other modes of representing or reproducing words or figures in a visible form…' this provision appears to admit electronic documents. Moreover, *Section 85 of the Evidence (Amendment) Act,* provides that the contents of a document may be proved as primary and secondary evidence. From this, it can be deduced that electronic documents in their original state constitute primary evidence, and when printed out, it may qualify as secondary evidence under *Section 87(b)* thereof.

Fundamentally, the current situation is slightly better than before, although the confusion still persists, although on a rather different scale. The *Advance Fee Fraud and other Fraud Related Offences Act*, in its import and practice, deals with offences that fall within the ambit of section 419 of the Nigerian Criminal Law Act which deals with the offences of obtaining by false pretense through different fraudulent schemes such as contract scam, credit card scam, inheritance scam, job scam, lottery scam, currency scam, marriage scam, immigration scam, counterfeiting, religious scam as well as cases of cyber-crime[400]. However the wording of the code does not provide a robust framework for the curtailing of cyber-crimes, as Law enforcement officers are limited in their prosecution of cyber-crimes for lack of specific

[396] Ikeh (note 393 above).
[397] ‗Although section 84 of the Evidence Act which governs affidavit evidence provides in clear terms that the court may permit an affidavit to be used notwithstanding' that it is ‗defective in form, if the court is satisfied that it has been sworn before a person duly authorized'. *F.B.I.R. v. Babaoye* (1974) 1 NMLR 136 (282-283, paras. G-A),as cited in *Colito v. Daibu* (2008) case no. CA/EL/11/2008, pg. 6, para 7, accessed at http://www.yusufali.net/reports/colito_v_daibu_nwlr.pdf, on the 24th October, 2014, at 2:28pm.
[398] Ikeh (note 393 above).
[399] Laws of the Federation of Nigeria.
[400] N, Ribadu, (Former Executive Chairman of the Economic and Financial Crimes Commission, EFCC, Nigeria) ‗Cybercrime and Commercial Fraud: A Nigerian Perspective' Modern Law for Global Commerce; Keynote address at the 40th annual session of UNCITRAL (Vienna, 2007), accessed at <http://www.uncitral.org/pdf/english/congress/Ribadu_Ibrahim.pdf> on 4th of March, 2013, at 03:06pm, 2.

legislation which covers the specified activity they purport to prosecute individuals for under the Section 419 provision. Section 419 provides:

> Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years. If the thing is of the value of one thousand naira or upwards, he is liable to imprisonment for seven years. It is immaterial that the thing is obtained or its delivery is induced through the medium of a contract induced by the false pretence. The offender cannot be arrested without warrant unless found committing the offence.

It is important to note that these disjointed pieces of legislation are inadequate, as there are matters which are left unregulated, such as information security, cyber-crimes content[401], data protection, and so on. This lacuna promotes uncertainty of the law[402]. In the light of this fact, certain issues arise, which need to be addressed. One of which is the question of whether a contract concluded by e-mail is capable of constituting a valid written contract in terms of the Statute of Frauds and other relevant legislation. Another is whether an electronic mark would constitute a valid signature fulfilling the requirement of signature under the current Laws.

The effect of Section 93 (2) of the Evidence (Amendment) Act clearly gives recognition to an electronic signature. It provides to the effect that where a rule of Law/Evidence stipulates the requirement of a signature, for the validity of a document ‗an electronic signature satisfies' this requirement[403]. Hence, it may be safely posited that an electronic signature suffices for the purpose of execution of an e-commerce transaction, provided that it is certified and

---

[401] Although the *Advance Fee Fraud and other Fraud Related Offences Act 2006* was enacted to tackle Cyber Crime in Nigeria, its efforts to check Cyber Crime have been hampered, due to the limited scope of this Law. Ibid.

[402] The Supreme Court of Nigeria's decision in *Anyaebosi v. R. T Briscoe Nigeria Ltd* [1987] 3 Nigeria Weekly Law Reports 84 (part 59) pg. 87 **is in conflict** with the Court of Appeal decision in *Nuba Commercial Farms Ltd v NAL Merchant Bank Ltd & anor* [2001] 16 NWLR 510 (part 740) on the issue of the admissibility of Computer print outs as evidence. While the Supreme Court viewed computer printouts as admissible albeit as secondary evidence, the Court of Appeal was of the view that the Evidence Act (s. 97) only provides for the admissibility of evidence in ‗book' form, and accordingly, held that computer printouts were inadmissible. Although the Court of Appeal decision is later in time than the Supreme Court decision, based on the doctrine of *stare decisis*, the Court of Appeal ought to have followed the earlier binding precedent established by the Supreme Court on the issue. Ewelukwa (note 384 above) 19. It is important to note that these decisions were made prior to the amendment of the evidence act, as the new Evidence (Amendment) Act, 2011 is worded to admit Computer printouts as evidence, as will be discussed later in this paper.

[403] Section 93 (2) Evidence Amendment Act, 2011.

accompanies the electronic communication[404]. The actual position is quite dicey, in the wake of the absence of specific legislation.

4.3.3 Implementation.

Addressing the implementation of the Nigerian Legislation pertaining to E-Commerce is rather unfeasible, owing to the absence of specific Legislation regulating e-commerce in the country, as noted above. However, the current situation in the country would be explored in chapter five below, in view of the recent development of the passing of an e-commerce bill in the republic, which is awaiting presidential assent[405].

4.4 The Developed Country under Review -The United Kingdom.

4.4.1 Introduction.

The United Kingdom has had a robust legislation regulating the use of computers and by extension - Cyber-crime, from as far back as the 1990s, titled *Computer Misuse Act, 1990* (CMA)[406]. Prior to the passing of this legislation, the turn of events revealed certain loopholes in the extant legislation[407], which led to calls for proactive legislation to curb the shortfall[408]. This led to the introduction of the Computer Misuse Act in 1990. A major case in point, which served as an impetus for the promulgation of this legislation is that of *R v. Gold & Schifreen*[409],

---

[404] Ikeh (note 393 above).

[405] E, Aginam, ‗At Last Senate Passes Cyber Crime Bill into Law', Vanguard Newspaper issue of 5 November, 2014, accessed http://www.vanguardngr.com/2014/11/last-senate-passes-cyber-crime-bill-law/, on the 27 November, 2014, 7:14am.

[406] F, Cassim, ‗Formulating Specialised Legislation to Address the growing spectre of Cybercrime: A Comparative Study' P.E.R, vol. 12, no. 4, 2009, accessed at http://www.nwu.ac.za/files/images/2009x12x4_Cassim_art.pdf on the 14th January, 2014, at 06:34pm, 36-79, at 47.

[407] The Forgery and Counterfeiting Act, 1981. The details of the loopholes are discussed further in footnote 109 below.

[408] Cassim, (note 406 above) 47.

[409](1988) 1 AC 1063. *Summary of R v. Schifreen & Gold case***:** Robert Schifreen and Stephen Gold, using conventional home computers and modems, gained unauthorized access to British Telecom's Prestel interactive view data service sometime between late 1984 and early 1985. While at a trade show, Shifreen had observed the username and password of a Prestel engineer. Based on this information, the pair explored the system and gained access to the login details of 50,000 Prestel customers including the personal message box of Prince Phillip, the Duke of Edinburg. Over time, Prestel got wind of the pair's activities, monitored their activities for some time, and consequently arrested them in the interest of national security. The pair was unable to be properly prosecuted as no relevant legislation existed to outlaw the unauthorized access to British Telecom's database. Instead they were tried under *Section 1 of the Forgery and Counterfeiting Act 1981* with defrauding British Telecom by manufacturing a ‗false instrument'. Their counsel appealed against the trial court's decision on grounds of insufficient evidence and with the claim that the forgery and counterfeiting act had been misapplied to their

in which the English courts concluded that their existing laws neither accommodated nor reflected the changes brought about by the computer technology[410].

In 2002, the UK published the *Electronic Commerce (EC Directive) Regulations,* with a guide. The Regulations are closely modeled after the EU E-Commerce Directive, 2000[411] and applies to virtually every online (e-commerce) business/commercial website[412]. The Directive was introduced in a bid to harmonise the rules regulating electronic commerce throughout Europe, to foster consumer confidence and repel uncertainty of the Law[413].

The CMA is the substantive legislation for the regulation of E-Commerce activities in the UK. The Computer Misuse Act made it a crime to access computer material without authorization, also known as hacking[414]. Other illegal actions include changing material on a computer without permission and hacking with the intent to commit some other crime[415]. It was consequently amended by certain sections of the Police and Justice Act, 2006[416] on the 11th of November, 2006[417]. The revised act combines the old Section 1 and Section 2 offences into a revised Section 1 and adds a new Section 3A offence of ‗Making, supplying or obtaining

---

conduct. They were acquitted and their acquittal was upheld by the House of Lords on the grounds that the existing legislation did not contemplate their conduct, as they had gained nothing from accessing the system and did not use data they encountered to commit an illegal act, which the current legislation provided for. The Computer Misuse Act, 1990, accessed at http://afmwebdesign.com/blog/?p=74, on the 27th August, 2014. See also http://itlaw.wikia.com/wiki/R_v_Gold_%26_Schifreen.

[410] http://www.legislation.gov.uk/ukpga/1990/18/contents.

[411] ‗The UK's E-Commerce Regulations' accessed at http://www.out-law.com/page-431, on the 9th May, 2014, at 4:53pm.

[412] Ibid.

[413] Further details pertaining to the European E-Commerce Directive are discussed in Chapter 3 above.

[414] Hacking generally refers to the unauthorised accessing of a computer system. However, the (CMA) law extends to all data and programs. Therefore, the changing, copying, moving, and removing of a computer program are all crimes under the Computer Misuse Act. Obtaining data from a computer system via hacking is also illegal, even if the information is not released or used in any way. ‗What was the purpose of the Computer Misuse Act 1990?' accessed at http://www.wisegeek.com/what-was-the-purpose-of-the-computer-misuse-act.htm, on the 28th August, 2014, at 1:24pm.

[415] Ibid.

[416] Specifically Sections 35 and 36 of the Police and Justice Act, 2006 amend Section 1and 3 of the Computer Misuse Act. See N, MacEwan, ‗The Computer Misuse Act 1990: Lessons from its past and Predictions for its future' Criminal Law Review, (2008) 1-9, 5, accessed at http://usir.salford.ac.uk/15815/7/MacEwan_Crim_LR.pdf, on the 16th August, 2014 at 10:36am.

[417] ‗UK bans denial of Service Attacks', The Register online issue of the 12th of November, 2006. Accessed at http://www.theregister.co.uk/2006/11/12/uk_bans_denial_of_service_attacks/, on the 27th August, 2014, at 1:49pm.

articles for use in computer misuse offences'[418]. Further details of the amendment would be discussed shortly.

4.4.2 The Law.

The discussions on the governing regime in the United Kingdom to be canvassed below would revolve around the CMA (as amended), as the EC Directive Regulations has been discussed at length in chapter 3. The amendment to the CMA sought to address two major challenges[419]. The first was the proliferation of Denial of Service (DoS) attacks[420] as well the creation and dissemination of hackers' tools[421]. The second was the need for the UK to fulfill its international commitments on cyber-crime[422], specifically, its ratification of the *Council of Europe's Convention on Cyber Crime (COECC)*.

The penalty for unauthorized access to a computer has been increased from 6 months' imprisonment to 2 years imprisonment[423]. Furthermore, the UK's introduction of an initiative, regarded as the 'National Hi-Tech Crime Unit' which is aimed at bringing the Police, members of the private sector and academics together, in an effort to jointly combat cyber-crime, is a laudable step[424].

The computer misuse act has many parts and sections; the main and basic sections are divided into- computer misuse offence, jurisdiction, miscellaneous and general[425]. Of interest to this discourse are the following salient sections under computer misuse offence rubric:

---

[418] 'Legislation and its Impact: The Impact of the Computer Misuse Act', accessed at http://www.sqa.org.uk/e-learning/ProfIssues02CD/page_08.htm, on the 16th August, 2014, at 10:37am.
[419] MacEwan (note 416 above) 1.
[420] Denials of Service (DoS) Attacks refer to premeditated onslaughts in which a web or electronic mail server is deliberately flooded with information to the point of collapse. 'These are launched against computer systems to cause loss of service to the users, typically the loss of network connectivity by consuming the bandwidth of the victim network or by overloading its computational resources'. See http://www.theregister.co.uk/2006/11/12/uk_bans_denial_of_service_attacks/, accessed on the 27th August, 2014, at 1:49pm; N, MacEwan, (note 416 above) 3.
[421] N, MacEwan, (note 415 above) 1.
[422] Ibid.
[423] Cassim, (note 406 above) 48.
[424] Ibid 48.
[425] Computer misuse act of british parliament | Law Teacher , accessed at http://www.lawteacher.net/technology-law/essays/computer-misuse-act-of-british-parliament.php , on the 27th of August, 2014 at 2:15pm.

Section 1: Unauthorised Access to Computer Material[426].

(1) A person is guilty of an offence if—
(a)he causes a computer to perform any function with intent to secure access to any program or data held in any computer [or to enable any such access to be secured] ;
(b)the access he intends to secure [or to enable to be secured,] is unauthorised; and
(c)he knows at the time when he causes the computer to perform the function that that is the case.
(2)The intent a person has to have to commit an offence under this section need not be directed at—
(a)any particular program or data;
(b)a program or data of any particular kind; or
(c)a program or data held in any particular computer.
(3)A person guilty of an offence under this section shall be liable—
(a)on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both…
(c)on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

It can be deduced from the above provisions that the unauthorised use of a computer system is prohibited, irrespective of whether the intention accompanying an unlicensed access to such computer system was directed at a particular program or data[427]. It is interesting to note that this provision, like the traditional criminal offences, fuses the requirement of a mental intention (mens rea)[428] to commit an act to coincide with the actual commission of the act (actus reus)[429], for a finding of liability[430]. Therefore, under the CMA, the actual act (actus reus) of unlawfully gaining access to a computer system in itself suffices, for a finding of guilt[431]. The operative phrase here appears to be ‗unauthorised' conduct.

[426] See appendix C below, for specific provisions of the CMA.
[427] Combined effect of Section 1 (1) and (2) CMA.
[428] This is an element of criminal responsibility, encompassing ‗guilty mind, a guilty or wrongful purpose; a criminal intent or guilty knowledge and willfulness'. More succinctly described as ‗a guilty mind or criminal intent in committing' an act. ‗A person's awareness that his/her conduct is criminal' satisfies the mental element, while ‗the act itself constitutes the physical element'. Accessed http://legal-dictionary.thefreedictionary.com/mens+rea, on 28 November, 2014 at 04:27pm.
[429] ‗The act or omissions that comprise the physical elements of a crime as required by statute'. Accessed at http://www.law.cornell.edu/wex/actus_reus, on 28 November, 2014 at 05:14pm.
[430] Accessed http://legal-dictionary.thefreedictionary.com/mens+rea, on 28 November, 2014 at 04:27pm.
[431] Section 1 (1) and (2) CMA.

Section 2: Unauthorised Access with intent to Commit or Facilitate Commission of Further Offences[432].

> (1)A person is guilty of an offence under this section if he commits an offence under section 1 above (~~–t~~he unauthorised access offence") with intent—
>
> (a)to commit an offence to which this section applies; or
>
> (b)to facilitate the commission of such an offence (whether by himself or by any other person);
>
> and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

This section combines a commission of the unauthorised conduct prohibited, in Section 1 above, with certain other prohibited acts ancilliary to it[433], such as aiding and abetting the commission of such unauthorised act(s). Furthermore, it relates to proscribed offences and to persons who have attained legal maturity and are first time offenders[434]. In addition, liability is strict, irrespective of whether the further offence is purported to be committed at a later date[435] or the commission of such further offence appears impossible[436].

Section 3: Unauthorised acts with intent to impair or with recklessness as to impairing operation of Computer, etc.

> (1) A person is guilty of an offence if—
>
> (a) he does any unauthorised act in relation to a computer;
>
> (b) at the time when he does the act he knows that it is unauthorised; and
>
> (c) either subsection (2) or subsection (3) below applies.
>
> (2)This subsection applies if the person intends by doing the act—
>
> (a) to impair the operation of any computer;

[432] See appendix C below, for specific provisions of the CMA.
[433] Section 2 (1) CMA.
[434] Section 2 (2) (a) and (b) CMA.
[435] Section 2 (3) CMA.
[436] Section 2 (4) CMA. See appendix C below, for specific provisions of the CMA.

(b) to prevent or hinder access to any program or data held in any computer;

(c) to impair the operation of any such program or the reliability of any such data; or

(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.

(3)This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.

Yet again, this provision fuses the unauthorised access offence, set out in section 1 with an anciliary act[437]. In this case, it pertains to the activity being matched with either an intention to impair the operation of the computer system or recklessness as to whether such act would in fact impair the operation of the computer system[438]. Here, the liability is equally strict.

Section 3A[439]:Making, supplying or obtaining articles for use in offence under Section 1 or 3.

(1)A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3.

(2)A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1 or 3.

(3)A person is guilty of an offence if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1 or 3.

(4)In this section ~~–a~~rticle" includes any program or data held in electronic form.

This provision outlaws the aiding and abetting of an attempt at committing any of the offences contemplated in either section 1 or 3 of the CMA[440]. In all the reviewed sections of the CMA,

[437] Section 3 (1) and (2) CMA.
[438] Section 3 (3) CMA. See appendix C below, for specific provisions of the CMA.
[439] Section 3A was introduced by Section 37 of the Police and Justice Act, 2006.
[440] Section 3A (1) CMA.

the maximum term of imprisonment is either twelve months or two years, depending on whether the conviction was based on summary proceedings or an indictment, respectively[441].

4.4.3 Implementation.

The application of the provisions of the CMA has been met with some criticism, as will be discussed shortly. This sub-head will be treated in line with certain cases in which the provisions of the CMA have been employed. Against the background of the Law Commission's declaration that the basic hacking offence in Section 1 of the CMA is principally aimed at the 'remote' hacker, although it was also 'apt to cover the employee or insider as well'[442]; One of the criticisms against the CMA is that its application to 'insiders' has been inconsistent and lacking in clarity[443].

One of the cases which brings to the fore the reasoning behind such criticism, is that of *DPP v. Bignell*[444]. Here, two police officers (Mr and Mrs Bignell), who were authorised to request information from the police national computer (PNC) for policing purposes only, requested a police computer operator, on six occasions, to obtain information from the PNC which, unknown to the operator, was for their own personal use. The Divisional Court held that the two officers had not committed a section 1 unauthorised access offence[445].

This paper respectfully disagrees with this interpretation by the Courts, the reason for this lies in the fact that the condition attached to their authority to obtain information from the PNC was 'for police purposes only'. Therefore, in the absence of such pre-requisite condition, their access to the information was clearly unauthorised for failure to satisfy the condition permitting the authority. Essentially, the permission relates not only to the area of conduct, but to the conduct within it. This reasoning is succinctly put by J.C Smith in his commentary of this case, in the following analogy: 'if I give you permission to enter my study for the purpose

[441] Section 3A (5) CMA. See appendix C below, for specific provisions of the CMA.
[442] MacEwan, (note 416 above) 2.
[443] Ibid.
[444] (1988) 1 Cr. App. R. 1.
[445] The Computer Misuse Act, 1990 accessed at http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/, on the 29th August, 2014 at 12:01pm.

of reading my books, your entering to drink my sherry would surely be unauthorised –access" to my sherry as well as my study'[446].

Furthermore, there has to be knowledge on the part of the offender that the access is unauthorised; mere recklessness is not sufficient[447]. This covers not only hackers but also employees who deliberately exceed their authority and access parts of a system officially denied to them[448]. This point is clearly elucidated in the case of *R v Bow Street Magistrates Court and Allison (AP)*[449], where the House of Lords considered whether an employee could commit an offence of securing _unauthorised access' to a computer contrary to section 1 CMA, it was held that the employee clearly came within the provisions of section 1 CMA as she intentionally caused a computer to give her access to data which she knew she was not authorised to access. Their Lordships made it clear that an employee would only be guilty of an offence if the employer clearly defined the limits of the employee's authority to access a program or data. It was hoped that this decision would review or even overturn the bignell decision, and provide clarity on the Court's stance on the matter for the purpose of promoting certainty of the Law. On the contrary, their lordships concluded that the bignell's decision was _probably right'[450].

It can be surmised that the CMA outlaws unauthorised access to data out rightly, irrespective of whether or not damage is caused as a result of such access, as clearly set out by section 1 of the Act. In terms of the provision of Section 2 which involves unauthorized access with the intent to commit or facilitate the commission of further offences, R v. Delamare[451] is instructive. In the instant case, the defendant worked in a bank, and was bribed with £100 to use the bank's computer system to obtain account details of 2 accounts[452]. He was found guilty of the charges, in breach of section 2 of the CMA, and charged with 4 months of detention, as

[446] (1998) Crim. L.R. 54. MacEwan, (note 416 above) 2.
[447] The Computer Misuse Act, 1990 accessed at http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/, on the 29th August, 2014 at 12:01pm.
[448] Ibid.
[449] *Ex parte Government of the United States of America (Allison)* [2002] 2 AC 216
[450] N, MacEwan,(note 416 above) 2.
[451] [2003] All ER (D) 127 (Feb).
[452] _Unauthorised Access to Computer Material', accessed at http://www.cps.gov.uk/legal/s_to_u/sentencing_manual/unauthorised_access_to_a_computer/, on the 29th August, 2014, at 12:43pm.

opposed to the previous 8 month sentence, on appeal, based on his youth and on account of him being a first time offender[453].

Another case of interest to this discourse pertaining to Section 2 CMA is that of *R v. Cropp*[454]. Here, the defendant ex-employee was alleged to have obtained a 70 percent discount, to which he was not entitled to, using a Point of Sale (POS)[455] terminal[456]. The judge acquitted the defendant in the belief that an offence was only committed if one computer is used to obtain material stored on another computer[457].

The third offence, set out in Section 3 of the CMA, is the _unauthorised modification of computer material.' This can be in the form of introducing viruses, corruption of programs or data and the deliberate deletion or stealing of confidential files or information. A case in point is that of *R v. Simon Vallor*[458], in which a web designer created three mass mailing viruses which were discovered to have infected 22,000 personal computers worldwide[459]. The defendant pleaded guilty and was sentenced to two years imprisonment for each of the three offences he committed[460].

The above cases raise the issue of the adequacy of the punishment in comparison to the extent of havoc caused. This leads to the ultimate question of the effectiveness of this piece of Legislation in prosecuting offenders and serving as a deterrent for prospective deviants. It is essential to reiterate that the Computer Misuse Act (1990) indeed contains a number of

---

[453] *R v. Delamare*, accessed at http://lexisweb.co.uk/cases/2003/february/r-v-delamare, on the 29th August, 2014, at 12:44pm.
[454] Snaresbrook Crown Court 05/07/1991 [1991] 7 CLSR 168, [1991] CL&P July/August 270 Computer Weekly 11 July 1992.
[455] A point of sale refers the physical location at which goods are sold to consumers. Often times, ~~t~~his is a standard cash register at the front of the store; in some cases, such as at a restaurant, the point of sale can be an electronic system which is used by the staff for multiple purposes, in this case including ringing up orders as well as generating the receipt and finalizing the purchase". Accessed http://www.investorwords.com/3725/point_of_sale.html#ixzz3JgCgAl40, 21 November, 2014, 7:55am.
[456] _Computer Misuse Act, 1990 Cases', accessed at http://www.computerevidence.co.uk/Cases/CMA.htm, on the 29th August, 2014, at 1:01pm.
[457] _Computer Misuse Act', accessed at http://www.lawteacher.net/criminal-law/essays/computer-misuse-act.php, on the 29th August, 2014, at 12:50pm.
[458] 2003 EWCA Crim. 2288.
[459] _Computer Misuse Act, 1990 Cases', accessed at http://www.computerevidence.co.uk/Cases/CMA.htm, on the 29th August, 2014, at 1:01pm.
[460] _Computer Misuse Act', accessed at http://www.lawteacher.net/criminal-law/essays/computer-misuse-act.php, on the 29th August, 2014, at 12:50pm.

significant flaws, as it fails to provide a complete answer to the issue of unauthorized access. However, its amendment tends to solve some of the unanswered problems inherent in the Act.

For instance, a UK court cleared a teenager named- David Lennon, in November 2005[461] on charges of sending five million emails[462] to his former employer – because the judge decided that no offence had been committed under the Act[463]. At this point, the need for the amendment of the CMA seemed quite apparent. Lennon's lawyer had successfully argued that the purpose of the company's server was to receive emails, and therefore the company had consented to the receipt of emails and their consequent modifications in data. The District Judge ruled that sending emails is an authorised act and that Lennon had no case to answer, so no trial took place. This ruling was subsequently overturned and Lennon was sentenced to two months' curfew with an electronic tag. This signifies a step in the right direction.

In view of the above interpretations of the law by the learned judges, it is pertinent to question whether judges possess specialist knowledge in computer operations to apply the Law and whether there exists a possibility of their misapplying the Law in certain circumstances. Perhaps this is the case. Essentially, the call for an amendment has been heeded in part, by the Police and Justice Act 2006. More recently, the cases churning out of the UK courts reflect a trend which denotes that the courts are grappling with cyber-crime matters with renewed understanding of the intricacies at play, rather than a rather hasty approach, as was seen previously.

4.4 Conclusion.

The common law has its limitations in terms of applicability and narrows significantly with regard to online crimes such as hacking, spamming, phishing, child pornography and the like.

[461] Lennon, Unreported, November 2 2005, Wimbledon Magistrates Court
[462] This is a case of Denial of Service (DoS) Attack, as discussed previously, see note 97 above.
[463] _UK bans denial of Service Attacks', The Register online issue of the 12th of November, 2006. Accessed at http://www.theregister.co.uk/2006/11/12/uk_bans_denial_of_service_attacks/, on the 27th August, 2014, at 1:49pm.

Cyber-crime laws function best within the framework of a clearly dedicated law and not as an appendage that allows remedies to fall short of liabilities[464].

A point which has been apparent throughout this continuum on the implementation of Electronic Commerce Laws is that having legislation is not enough, because it is susceptible to being outdated over time. Rather, concerted efforts by stakeholders, in terms of awareness, sensitization, amendments (where required), training personnel and a robust implementation regime is key to fighting the menace of Cyber-crime and enabling the benefits inherent in E-Commerce outshine the demerits which may encroach on its existence.

[464] Nuhu Ribadu, (Former Executive Chairman of the Economic and Financial Crimes Commission, EFCC, Nigeria) _Cybercrime and Commercial Fraud: A Nigerian Perspective' Modern Law for Global Commerce; Keynote address at the 40th annual session of UNCITRAL (Vienna, 2007), accessed at <http://www.uncitral.org/pdf/english/congress/Ribadu_Ibrahim.pdf> on 4th of March, 2013, at 03:06pm, 1.

CHAPTER FIVE: COMPARATIVE ANALYSIS & CONCLUSION.

5.1 Introduction: Comparative Study.

As alluded to in the preceding chapters, various nations have different legislation regulating e-commerce activities. While some of these legislations are specifically developed to police e-commerce activities, like in the case of South Africa and the United Kingdom; some others are not, like in the case of Nigeria. The core objective of this chapter is to assess the efficacy of the regulations in place to regulate e-commerce activities in the various countries under review, in view of the shortfalls highlighted previously.

In essence, the goal of this chapter is to determine whether the existing laws are relevant to tackle the matters they were promulgated to address. Furthermore, an inquiry of the extent to which these laws achieve their purpose(s), will be embarked upon. In addition, what may be done to promote their efficiency, as well as suggestions as regards a way forward will be explored, by way of recommendations. The aim of this chapter is to firstly make a comparative analysis of the existing legal regimes. Secondly, an evaluation of the effectiveness of these regimes would be embarked upon. Thirdly, recommendations would be proffered and a conclusion would be reached accordingly. At this point, a cursory look at the merits and demerits of the substantive legislation regulating e-commerce in South Africa is apposite.

5.2 Effectiveness- merits and demerits.

The E-commerce Legal Regimes in the countries under review are at different spheres of operation. However, a lot can be gleaned from their dynamics. While the regime in the United Kingdom has been in operation for the longest period, amongst the countries under review, that of South Africa follows next. These two countries have their e-commerce legal regimes in full-fledged operation, while that of Nigeria has barely started off. Against this background, Nigeria, South Africa and several other African Countries have a lot to learn from the experience of the United Kingdom.

The South African and United Kingdom regimes are similar to the extent that they have operational e-commerce legal regimes, while Nigeria has a new legal regime which is not yet fully functional. The merit of this is that the mistakes made previously by the other two

regimes, which shape their current regime may be taken into account by Nigeria, in forming a formidable regime to suite her peculiarities.

Furthermore, the salient issues of writing, signatures and originality which the Nigerian Cybercrime Bill has omitted to address, may be addressed in line with how South Africa Addresses these issues in her ECTA. In addition, the UK's approach in introducing a new criminal liability class to prosecute persons who commit crimes as an organized group, owing to the trend of prevalence of organized cyber-crimes, is instructive.

While, South Africa adopts an approach of dealing with the issue of Jurisdiction as being vested on a South African court in a number of occasions[465], as highlighted above, which practice has been identified by this thesis as problematic and in need of an amendment; the English legislation vests jurisdiction on English Courts where there exists one significant link with the domestic jurisdiction of England or wales. This is a more practical approach, as it automatically lays to rest the query of which court or district is vested with Jurisdiction, which the ECTA raises. Rather, the district court of the domestic jurisdiction linked with the matter automatically assumes jurisdiction. These matters amongst others, would be further analysed below.

5.2.1 South Africa

As noted in the previous chapters, the Electronic Communications and Transactions Act (ECTA) is the chief legal instrument which regulates e-commerce activities in South Africa. As has been noted in the foregoing chapter, the ECTA gives legal recognition to data messages[466] and prohibits discrimination against the admissibility of documents on the grounds of its (electronic) form[467]. In addition, it (the ECTA) sets down rules for the validity of a data message as written[468], as being signed[469] and as an original[470] respectively. It also outlaws cyber-crime in chapter XIII[471]. The effect of these provisions is that it gives legal certainty in terms of electronically concluded contracts and forms a solid background for e-commerce.

[465] *Section 90 ECTA.*
[466] *Section 11 (1) ECTA.*
[467] *Section 11 ECTA.*
[468] *Section 12 ECTA.*
[469] *Section 13 ECTA.*
[470] *Section 14 ECTA.*
[471] See page 62 above.

Moreover, the provisions proscribing cyber-crime activities, affords some assurances of a measure of security as regards e-commerce transactions and encourages increased participation in e-commerce ventures.

Furthermore, an interesting element of the ECTA is that it empowers cyber-inspectors to enter any premises to access information which may impact upon their investigation into cyber-crime[472]. However, this provision may likely infringe on the right to privacy[473] guaranteed by the constitution, thereby rendering this particular provision invalid due to its inconsistency with the constitution[474], by virtue of the supremacy clause of the constitution[475]. Another demerit of the ECTA is that the sanctions it imposes are not severe enough to serve as a deterrent to crimes[476]. Now, this goes to the heart of the inquiry of this chapter, as one can put forward the argument that any legislation which lacks the force to compel obedience can scarcely be qualified as effective in the least sense of the word.

Additionally, in view of the highlighted shortcomings of the ECTA, the Electronic Communications and Transactions Act Amendment Bill 2012 seeks to introduce the following major amendments to the current ECTA:

- It proposes to increase the sanction imposed for the contravention of Section 86 (1), (2) and (3) of the ECTA from a maximum period of 12 months imprisonment to a maximum term of 10 years imprisonment or a fine of R10,000,000[477];

- It proposes to increase the sanction imposed for the contravention of Section 87 (1), (2) and (3) of the ECTA from a maximum period of 12 months imprisonment to a maximum period of 5 years imprisonment or a fine of R5,000,000[478];

---

[472] *Section 82 ECTA.*
[473] *Section 14* of the Constitution of the Republic of South Africa, 1996.
[474] The Constitution of the Republic of South Africa, 1996.
[475] *Section 2* of the Constitution of the Republic of South Africa, 1996 provides: ―This Constitution is the supreme law of the Republic; law or conduct inconsistent with it is invalid, and the obligations imposed by it must be fulfilled".
[476] See note 343 above, and paragraph 4.2.4.3 above.
[477] *Section 86 (6)* ECTA Amendment Bill, 2012, accessed at file:///C:/Users/user/Downloads/electronic%20communications%20and%20transactions%20amendment%20bill%202012%20(1).pdf, on the 5th September, 2014 at 8:32pm.
[478] *Section 87 (3) ECTA Amendment Bill, 2012.*

- The bill also proposes that anyone who aids and abets or attempts at committing a crime in terms of Section 88 ECTA may be liable to a maximum period of 5 years imprisonment or a fine of R5,000,000[479].

On face value, these provisions seem to cater for the shortfall of inadequacy of penalty to injury caused, discussed above. Although, the efficacy of these provisions is yet to be tested by case law, thus only time will tell how it will be applied by the courts.

On a final note, in terms of jurisdiction, the ECTA provides that a South African court can exercise jurisdiction, when[480]:

a) the cause of action takes place in the republic[481];
b) where the preparatory acts leading to offence took place in the republic or where the offence had an effect in the republic[482];
c) where the offence was committed by a south African Citizen or Permanent Residence holder or a person carrying on business in the republic[483] ; or
d) where the offence was committed in an aircraft or ship registered in the republic, or on a flight or voyage to or from the republic[484].

It is submitted that these provisions, despite their lofty ideals, are inchoate and are at variance with the provision of *Section 28 (1) (d)* of the Magistrate Court Act[485], which requires ‗the whole cause of action' to take place within a particular court or district, for the determination of jurisdiction. In view of this, if the provisions of the ECTA conferring jurisdiction on South African Courts in terms of offences committed abroad, are to be implemented, the question arises as to which particular regional or district court has jurisdiction to hear the matter.

Although a look at the wording of *section 28(1) (d)* of the Magistrate Court Act[486] reveals that it gives room for additional jurisdiction to be granted to a court by another Law, for instance, the ECTA. However, the ECTA appears to require the conferral of jurisdiction to a certain

[479] *Section 88 (1) ECTA Amendment Bill, 2012.*
[480] *Section 90 ECTA.*
[481] *Section 90(a) ECTA.*
[482] *Section 90(b) ECTA.*
[483] *Section 90(c) ECTA.*
[484] *Section 90(d) ECTA.*
[485] 32 of 1944. *Section 28(1) (d)* provides: ‗Saving any other jurisdiction assigned to a court by this Act or by any other law, the persons in respect of whom the court shall… have jurisdiction shall be the following and no other:… (d)any person, whether or not he or she resides, carries on business or is employed within the district or regional division, if the cause of action arose wholly within the district or regional division'.
[486] Ibid.

court(s) in terms of the causes of action which arise abroad, in order to give effect to this new addition to the existing Law. Rather, the ECTA, simply prescribed additional jurisdiction, in terms of causes of action arising abroad, without stating precisely what circumstances would qualify a court with jurisdiction or which court would be vested with jurisdiction to entertain the matter.

From the continuum it can be inferred that the ECTA is a viable instrument which is capable of effectively regulating e-commerce activities in the republic, although it includes certain shortfalls, which are incapable of overriding its objects, though such shortfalls require attention timeously.

5.2.2 Nigeria.

Nigeria presents quite a peculiar case study, as it is a developing country struggling with several socio-economic problems ranging from poverty[487], to corruption, to terrorism among other problems. In addition to these, it is contending with the menace of cyber-crimes. Moreover, it neither has specific legislation to curb this threat to her national security, nor legislation to regulate e-commerce activities in the republic. In Nigeria, the law enforcement agencies and the criminal justice system are astounded by the nature and extent of cyber-crime, which intricacies are incomprehensible to them[488].

Furthermore, the instances of cyber-crime are largely unreported; hence, the cases are more rampant than stated[489]. As if that is not enough, the judges and prosecutors are ill equipped to grapple with the situation, as they are unable to swiftly keep up pace with the technology by

[487] Daily Independent Editorial, ―World Bank Report on Poverty in Nigeria", May, 2014, accessed http://dailyindependentnig.com/2014/05/world-bank-report-poverty-nigeria/ on 21 November 2014 at 8:25am (discusses the irony of Nigeria being recently declared by the National Bureau of Statistics to have a Gross Domestic Profit of $510 billion dollars, making her the largest economy in Africa, and the 26th largest in the world; in sharp contrast with a world bank assessment of poverty in Nigeria, rating her third among the world 10 countries with cases of extreme poverty); Poverty Reduction & Equity, publication of the world Bank,―Nigeria: Poverty in the Midst of Plenty: A Challenge of Growth and Inclusion" 1996, accessed http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTPOVERTY/EXTPA/0,,contentMDK:20204610~menuPK:435735~pagePK:148956~piPK:216618~theSitePK:430367,00.html, on 21 November 2014 at 8:35am (traces the problem of poverty in Nigeria to a sharp increase in population and lack of proper management of resources) .

[488] Nuhu Ribadu, (Former Executive Chairman of the Economic and Financial Crimes Commission, EFCC, Nigeria) ‗Cybercrime and Commercial Fraud: A Nigerian Perspective' Modern Law for Global Commerce; Keynote address at the 40th annual session of UNCITRAL (Vienna, 2007), accessed at <http://www.uncitral.org/pdf/english/congress/Ribadu_Ibrahim.pdf> on 4th of March, 2013, at 03:06pm, 2.

[489] Ibid.

matching crime with appropriate punishments, in the absence of relevant legislation[490]. What applies in Nigeria however is that various disjointed pieces of predominantly obsolete Legislations collectively regulate various spheres of activity, including e-commerce. Rather, what is needed is a legal framework which harmonises the regulation of the entire gamut of e-commerce activity, inclusive of cyber-crimes and paves way for the legal recognition of documents/materials in the electronic form, in order to ensure legal certainty.

For instance, Commerce in Nigeria today, is generally still regulated by the *Sale of Goods Act of 1893*. The Sale of Goods Act became applicable in Nigeria, by virtue of its incorporation into Nigerian Law, with other Statutes of General Application in England, in force before the 1st of January 1900 in the United Kingdom[491]. It goes without saying this act is archaic, hence, can hardly cater for e-commerce challenges, much less, regulate it effectively. This presents a clear picture of the nature of the problem.

Against this background, calls have been made from various quarters of the economy, clamoring for new legislation to address the growing spectre of cyber-crimes, and e-commerce generally in Nigeria[492]. In response, various bills have been sponsored over the years[493], the latest of which is the Cybercrime Bill 2013[494], which had previously been reported to have been sent to the National Assembly for onward transmission into Law[495]. More recently, it has

---

[490] Ibid.

[491] D, Enedeghe, –Comparative Legal Analysis of the Applicable Legal Protection for Purchasers on the Internet in Europe and the USA-Lessons for Nigeria", Central European University, Budapest, Hungary, LLM Thesis, 29th March, 2013, pg 1-59, at 44, accessed at http://www.etd.ceu.hu/2013/enadeghe_deborah.pdf&sa=U&ei=trw_VIThC5GS7AbPvoDQCg&ved=0CE0QFjAJ&usg=AFQjCNFD7CgiCanJqaj-qUSCztSHLdwvoQ, on the 16th October, 2014, at 2:48pm.

[492] Ibid, 45, such as the Supreme court, the federal ministry of justice the Nigerian Bar Association, and so on.

[493] Some of which include the Computer Security and Critical Information Infrastructure Protection Bill 2005 (sponsored by the Executive), the Cyber Security and Data Protection Agency (Establishment, etc) Bill 2008 (sponsored by Hon. Bassey Etim), the Electronic Fraud Prohibition Bill 2008 (sponsored by Senator Ayo Arise), the Nigeria Computer Security and Protection Agency Bill 2009 (another executive bill), the Computer Misuse Bill 2009 (sponsored by Senator Wilson Ake) and the Economic and Financial Crimes Commission Act (Amendment) Bill 2010 (sponsored by Hon. Abubakar Shehu Bunu'), as recounted by Dr. N, Ewelukwa in E, Nkanga, –Non-Passage of Cyber Crime Bill Decried", Thisday Live, online news article of 31st March, 2011, accessed at http://www.thisdaylive.com/articles/non-passage-of-cyber-crime-bill-decried/88750/, on the 17th October, 2014, at 2:00pm.

[494] The long title is "the Bill for an Act to Provide for the Prohibition, Prevention, Detection, Response and Prosecution of Cyber Crimes and Other Related Matters 2013".

[495] C, Okafor, –Jonathan Sends Cybercrime Bill to Senate", Daily Independent Online News Article of the 22nd January, 2014, accessed at http://dailyindependentnig.com/2014/01/jonathan-sends-cybercrime-bill-to-senate/, on the 30th October, 2014 at 9:55am; P, Adepoju, –Nigerian Government Seeks to Monitor and Control Cyber Space with New Law", Humanipo online issue of the 30th August, 2013, accessed at

been reported to have been passed into law by the Senate, and is currently awaiting presidential assent[496]. The previous bills were rejected for one reason or the other, one of which was the fact that its provisions duplicated the functions of existing Law enforcement agencies in Nigeria[497].

The Cyber Crime Bill 2013 had generated a lot of discussion[498] and it was earnestly hoped that this bill would actually be passed into Law, unlike its predecessors, which were relegated to the wayside[499]. Particularly due to the fact that this is a much awaited Legislation, which is long overdue[500]. For instance, in 2012, it was reported that the Economic and Financial Crimes Commission (EFCC) in Nigeria, had made 288 cyber-crime related arrests, but a staggering 234 of these cases were pending, in the absence of cyber-crime Legislation to prosecute them[501]. Further, it is reported that Nigeria's lack of legislation proscribing cyber-crimes makes

---

http://www.humanipo.com/news/30907/nigerian-government-seeks-to-monitor-and-control-cyberspace-with-new-law/, on the 17th October, 2014, at 2:20pm.

[496] E, Aginam, "At Last Senate Passes Cyber Crime Bill into Law', Vanguard Newspaper issue of 5 November, 2014, accessed http://www.vanguardngr.com/2014/11/last-senate-passes-cyber-crime-bill-law/, on the 27 November, 2014, 7:14am.

[497] D, Enedeghe, "Comparative Legal Analysis of the Applicable Legal Protection for Purchasers on the Internet in Europe and the USA-Lessons for Nigeria", Central European University, Budapest, Hungary, LLM Thesis, 29th March, 2013, pg 1-59, at 45, accessed at http://www.etd.ceu.hu/2013/enadeghe_deborah.pdf&sa=U&ei=trw_VIThC5GS7AbPvoDQCg&ved=0CE0QFjAJ&usg=AFQjCNFD7CgiCanJqaj-qUSCztSHLdwvoQ, on the 16th October, 2014, at 2:48pm.

[498] See generally- E, Ebhota, "Nigerians React to Cyber Crime Bill", Daily Trust Online News Article of 2nd Februaury, 2014, accessed at http://allafrica.com/stories/201402031339.html, on the 17th October, 2014, at 2:40pm; S, Opara, "Cyber-Crime: Nigeria Redeems Image", in the Punch Online Newspaper issue of the 22nd October, 2013, accessed at http://www.punchng.com/business/technology/cyber-crime-nigeria-moves-to-redeem-image/, on the 17th October, 2014, at 2:43pm.

[499] E, Nkanga, "Non-Passage of Cyber Crime Bill Decried", Thisday Live, online news article of 31st March, 2011, accessed at http://www.thisdaylive.com/articles/non-passage-of-cyber-crime-bill-decried/88750/, on the 17th October, 2014, at 2:00pm.

[500] E, Aginam, "Nigeria: Fresh Worry over Non-Passage of Cyber Security Bill to Curb E-Fraud", Vanguard Newspaper online issue of the 27th July, 2014, accessed at http://allafrica.com/stories/201407280149.html, on the 17th October, 2014, at 2:54pm; E, Okutuyi, "Nigeria Not Ready to Fight Cyber Crime", Premium Times online issue of the 12th, March, 2013, accessed at https://www.premiumtimesng.com/news/124330-nigerian-not-ready-to-fight-cyber-crime-ncc.html, on the 17th October, 2014, at 3:00pm; "Report on Cyber Threat Calls for quick passage of 2012 Bill", Nigeria News Digest, 8th May, 2014 issue, accessed at http://nigerianewsdigest.com/%EF%BB%BFreport-on-cyber-threat-calls-for-quick-passage-of-2012-bill/, on the 17th October, 2014, at 3:03pm.; K, Goodie, "Non-Passage of Cyber Security Bills Cripple Mobile Money", Biztech Africa's Online issue of the 6th September, 2014, accessed at http://www.biztechafrica.com/article/non-passage-cyber-security-bills-cripples-mobile-m/8727/, on the 17th October, 2014, at 3:07pm.

[501] R, Akinwunmi, "Rep Passes Ant-Cybercrime Bill for Second Reading", Daily Independent News Article published on the 27th November, 2012, accessed at http://dailyindependentnig.com/2012/11/rep-passes-anti-cybercrime-bill-for-second-reading/ on the 24th October, 2014 at 3:21pm.

it a preferred destination, more like a haven for cyber criminals to practice their degenerate activities unbridled[502].

The comparative analysis on Nigeria will be conducted in terms of her current situation (-lack of specific legislation)[503], although reference to the provisions of the bill will be made, when required. In view of the foregoing, Nigeria as a case study, presents a clear picture of how severely lack of specific Legislation regulating e-commerce and by extension- outlawing e-commerce related criminal activities can cripple an economy.

However, the Cybercrime Bill appears to offer some solutions to the current problems pertaining to e-commerce in the country[504]. The objectives of the bill include, among other goals, protecting Nigeria's national information structure and establishing an integrated legal, regulatory, and institutional framework to deal with cyber-crimes[505]. The Bill proposes to criminalise several nefarious activities, not outlawed previously, notably:

- Offenses against what the legislation calls the ‗critical national information structure'.[506] Critical national information structure includes any and all computer systems, networks, and information infrastructure designated as such by the country's president on the recommendation of the national security advisor[507]. A person who commits any offense under the legislation (including the offenses stipulated below) involving a critical national information structure would, on conviction, receive a sentence ranging from 15 years to the death penalty, depending on the gravity of the offense[508].
- In addition, the legislation proposes to establish numerous other crimes, including: obtaining unlawful access to a computer[509], unlawful interception of

[502] E, Aginam, ―Nigeria: Fresh Worry over Non-Passage of Cyber Security Bill to Curb E-Fraud", Vanguard Newspaper online issue of the 27th July, 2014, accessed at http://allafrica.com/stories/201407280149.html, on the 17th October, 2014, at 2:54pm
[503] In the absence of Presidential Assent to the bill, the bill is yet to become operational.
[504] See appendix B below, for specific provisions of the Cybercrime Bill.
[505] Section 1 Cybercrime Bill 2013.
[506] Global Legal Monitor: ‗Nigeria: Cybercrime Bill Proposed', accessed at http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403853_text, on the 23rd October, 2014, at 11:28am.
[507] Section 3 Cybercrime Bill 2013. Ibid.
[508] Section 5 Cybercrime Bill 2013.
[509] Section 6 Cybercrime Bill 2013.

communications[510], unauthorized modification of a computer program or data[511], system interference[512], misuse of devices[513], computer-related forgery[514], computer-related fraud[515], identity theft or impersonation[516], child pornography[517], cyber stalking[518], and cybersquatting[519].

- Another notable provision in the legislation is that which proposes to outlaw cyber terrorism, and sets a penalty of life imprisonment for anyone found guilty of this crime[520]. Racist and Xenophobic tendencies are also proscribed in Section 18.
- A provision of this bill, which has generated much disquiet amongst the Nigerian populace[521], is that which requires Internet and phone service providers to retain and make available to government agencies, customer information, including traffic data as well as subscriber information[522]. If a service provider fails to cooperate with government agencies in this regard, it would be subject to a fine of at least ₦10 million, and its director/manager/officer would be prosecuted and, on conviction, be subject to at least three years in prison and/or a ₦7 million fine[523].

[510] Section 7 Cybercrime Bill 2013.
[511] Section 8 Cybercrime Bill 2013.
[512] Section 9 Cybercrime Bill 2013.
[513] Section 10 Cybercrime Bill 2013.
[514] Section 11 Cybercrime Bill 2013.
[515] Section 12 Cybercrime Bill 2013.
[516] Section 13 Cybercrime Bill 2013.
[517] Section 14 Cybercrime Bill 2013.
[518] Section 15 Cybercrime Bill 2013.
[519] Section 16 Cybercrime Bill 2013.
[520] Section 17 Cybercrime Bill 2013.
[521] E, Ebhota, "Nigerians React to Cybercrime Bill", Daily Trust Online News Article of 2nd Februaury, 2014, accessed at http://allafrica.com/stories/201402031339.html, on the 17th October, 2014, at 2:40pm; P, Adepoju, "Nigerian Government Seeks to Monitor and Control Cyber Space with New Law", Humanipo online issue of the 30th August, 2013, accessed at http://www.humanipo.com/news/30907/nigerian-government-seeks-to-monitor-and-control-cyberspace-with-new-law/, on the 17th October, 2014, at 2:20pm; Z, Adaramola, "Is 'Wire-tap' Law meant to Stifle Free Speech or Fight Cyber Crimes?", Daily Trust IT Law Article, published on the 18th November, 2013, accessed at http://www.dailytrust.com.ng/daily/it-world/10192-is-wire-tap-law-meant-to-stifle-free-speech-or-fight-cybercrimes, on the 23rd October, 2014, at 1:00pm; A, Bamgboye, "Lawyers React on Cybercrime Bill", Daily Trust News Article, Published on the 29th of January, 2014, accessed at http://www.dailytrust.com.ng/daily/news/15545-lawyers-react-on-cyber-crime-bill, on the 23rd October, 2014, at 11:29pm; "The Bugging Bill", Daily Trust Editorial Article, published on the 7th February, 2014, accessed at http://www.dailytrust.com.ng/daily/editorial/16307-the-bugging-bill, on the 23rd October, 2014, at 1:35pm.
[522] Section 21 Cybercrime Bill 2013. This provision is also likely to deter foreign investment in the Republic.
[523] Section 21(6) & 23 Cybercrime Bill 2013.

- The legislation would also afford law enforcement officers broad search, arrest, and seizure powers, including some that do not require judicial oversight[524]. This occurs when there is what the legislation terms a "verifiable urgency' that a cybercrime is about to be committed or that there is an "urgent need to prevent the commission of an offence', and obtaining a warrant would take time and be prejudicial to public safety or order[525]. In such a circumstance, a law enforcement officer would have the authority to enter any premises or vehicle that he reasonably suspects is being used or is likely to be used for the commission of a crime or that contains evidence of the commission of a crime[526]. Once in control of the premises or vehicle, the officer need not wait to obtain a warrant; he may conduct searches, seize items, or arrest persons he "reasonably suspects' to be connected to the crime[527].

In view of the laudable objectives of the Cybercrime Bill discussed above, one merit which this thesis submits as inclining to stick out the most, is the fact that it tends to cover the field, in terms of what had been previously lacking in Legislation, to effectively deter cyber-crimes and restore confidence in e-commerce methods of contracting. However, this bill has the propensity to be subjected to abuse by security agents, and be used as a tool to stifle free speech by political power holders[528]. Hence, great caution should be taken and stringent conditions should be imposed on its use, to check possible abuse. In fact, some schools of thought hold the view that blanket monitoring of consumers, through internet and mobile service providers, as discussed above, should be discouraged altogether[529].

---

[524] Global Legal Monitor: "Nigeria: Cybercrime Bill Proposed', accessed at http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403853_text, on the 23rd October, 2014, at 11:28am.
[525] Section 28 Cybercrime Bill 2013.
[526] Section 28 Cybercrime Bill 2013. Global Legal Monitor: "Nigeria: Cybercrime Bill Proposed', accessed at http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403853_text, on the 23rd October, 2014, at 11:28am.
[527] Ibid.
[528] Z, Adaramola, "Is "Wire-tap' Law meant to Stifle Free Speech or Fight Cyber Crimes?", Daily Trust IT Law Article, published on the 18th November, 2013, accessed at http://www.dailytrust.com.ng/daily/it-world/10192-is-wire-tap-law-meant-to-stifle-free-speech-or-fight-cybercrimes, on the 23rd October, 2014, at 1:00pm;
[529] A, Bamgboye, "Lawyers React on Cybercrime Bill", Daily Trust News Article, Published on the 29th of January, 2014, accessed at http://www.dailytrust.com.ng/daily/news/15545-lawyers-react-on-cyber-crime-bill, on the 23rd October, 2014, at 11:29pm.

The provision of *Section 21 of the Cybercrime Bill*, which permits service providers to retain ‗traffic data, subscriber information and related content'[530] and ‗release such information at the request of relevant authorities'[531], requires such information to be treated with utmost confidentiality with regard to individuals' right to privacy enshrined in the Nigerian Constitution[532]. Essentially, this provision, just like its South African counterpart (*Section 82 of the ECTA*), despite the fact that the constitutional right to privacy was mentioned in this bill, (which was not the case with the ECTA Legislation), it is not absolved from the susceptibility to infringe on the right to privacy[533] guaranteed by the constitution. Therefore, in view of the derogation this particular provision contemplates, it is thereby rendered void to the extent of its inconsistency, by virtue of the supremacy clause of the constitution[534].

In conclusion of the discourse on the effectiveness of the e-commerce Legal regime in Nigeria, it is important to note that the above discussed bill is anticipated to go a long way in functioning as an effective ameliorant to Nigeria's current lack of specific regulation governing her e-commerce regime. However, the possibility of the *Cybercrime Bill* making an impact is largely dependent on the assent of this Bill by Nigeria's President. This brings us back to where Nigeria currently stands - lack of proper regulation of e-commerce activities. As indicated in chapter 4, above, Nigeria's current *Evidence (Amendment) Act*[535] recognises paper-based and electronic documents alike[536], as a document is defined to encompass[537]:

---

[530] Section 21 (1) Cybercrime Bill, 2013. This provision has been interpreted to include: personal emails, text messages, voice conversations, fax, instant messages, voice mails and other forms of multimedia messages. ―The Bugging Bill", Daily Trust Editorial Article, published on the 7th February, 2014, accessed at http://www.dailytrust.com.ng/daily/editorial/16307-the-bugging-bill, on the 23rd October, 2014, at 1:35pm.

[531] Section 21 (2) Cybercrime Bill, 2013.

[532] *Section 37 of the 1999 Constitution of the Federal Republic of Nigeria* provides: ―The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected."

[533] *Section 37 of the 1999 Constitution of the Federal Republic of Nigeria.*

[534] *Section 1 (3) of the 1999 Constitution of the Federal Republic of Nigeria* ―If any other law is inconsistent with the provisions of this Constitution, this Constitution shall prevail, and that other law shall, to the extent of the inconsistency, be void".

[535] Act No. 18 of 2011.

[536] Section 258 *Evidence (Amendment) Act*, Definition of document (a) & (b).

[537] The choice of the word ‗encompass' denotes that the definition given should not be limited, but rather, it includes a wide range of other things not mentioned.

> ‗any device by means of which information is recorded, stored or retrievable including computer output'[538].

However, Nigerian Law requires certain documents to be evidenced in writing and signed for them to be valid[539]; this rule is still applicable in the absence of any regulation to counter this obsolete piece of legislation, considering the current e-commerce trends. The problem of inadequacy of existing legislation to curb certain vices, such as cyber-crimes are expected to be addressed by the *Cybercrime Bill 2013*, although the issue of signature, writing and originality are not fully addressed by the Bill. In the light of this, it is proposed that the bill be passed into Law speedily and the issues of writing, signature and originality are addressed by way of an amendment, in line with the letter of the model law[540], with the due consultation with experts skilled in ICT[541].

5.2.3 United Kingdom.

As discussed previously in the United Kingdom, the Computer misuse Act (CMA), 1990 is the substantive legislation governing e-commerce activities. Section 1 of the CMA, criminalises the unauthorised access to a computer material[542] or a person's user identity and password. While a Section 2 offence, is slightly more serious, as it relates to committing further crimes after gaining unauthorised access to another's computer[543], as is provided in terms of section 1. This may include stealing money by gaining unlawful access to another's computer or using information discovered during an unsanctioned use of another's system to blackmail them[544]. Offences proscribed in Section 3 include spreading viruses, deleting files, using Trojans to

---

[538] Section 258, Definition of document (b).

[539] For instance, *Section 4, Statute of Frauds, 1677* states that proceedings to enforce a contract for sale of land can only be brought where the contract or some memorandum or note of it, is in writing and signed by the person against whom the action is brought or that person's authorized agent. E, Ikeh, ‗Towards a Legal Framework for the Development of E-Commerce in Nigeria: Issues and Prospects' February 2014, accessed at http://www.mondaq.com/x/294344/Contract+Law/Towards+A+Legal+Framework+For+The+Development+Of+ECommerce+In, on the 6th of September, 2014 at 5:28pm.

[540] The (United Nations' Commission on International Trade Law) UNCITRAL Model Law on Electronic Commerce, 1996.

[541] Information and Communication Technology.

[542] *Section 1 CMA.*

[543] Section 2 CMA.

[544] O, Solon, ―UK Law introduces Life Sentences for Cyber Criminals", wired.co.uk online Politics Issue of the 6th June, 2014, accessed at http://www.wired.co.uk/news/archive/2014-06/06/cybercrime-bill-life-sentence, on the 27th October, 2014.

steal data or mounting a denial of service attack[545], and the maximum sentence for these offences is ten years imprisonment[546]. In addition, an amendment introduces Section 3A[547], which proscribes generally, the making, supplying or obtaining materials for use in the commission of the offences set out in Sections 1 or 3 of the CMA.

More recently, the *'Serious Crime Bill'* which was introduced to the House of Lords on the 5th June, 2014, is proposed to amend the CMA further, by adding the offence rubric _Unauthorised acts causing serious damage'[548]. This offence is proposed to cover attacks that could result in loss of life, serious injury, social disruption or damage to the economy, or pose a threat to the environment or national security[549]. Some of the aims of the bill include improving the UK Government's ability to recover criminal assets, amending _the Computer Misuse Act 1990 to ensure sentences for attacks on computer systems fully reflect the damage they cause' and creating _a new offence targeting people who knowingly participate in an organised crime group'[550]. This is a pro-active step, in view of the fact that lately, cyber-crime is scarcely committed by lone individuals, but rather by a group of individuals, this fact is evident from case law[551].

Moreover, it is trite that the issue of Jurisdiction is a well mooted subject, in terms of e-commerce transactions (as is evident in the discourse on South Africa). The approach adopted by the CMA in addressing trans-border crimes is of interest to this discourse, in view of the inherent nature of e-commerce to virtually break down territorial borders. Prior to the advent of the CMA, the English Appeal Court in 1985 indicated that if a person sent a message from London to divert funds from New York to his accounts in Geneva, the theft would not have

---

[545] *Section 3 CMA.*
[546] Solon, (note 543 above).
[547] Introduced by Section 37 of the Police and Justice Act, 2006.
[548] _The Serious Crime Bill and Related Material', Equality and Diversity Forum online issue of the 23rd October, 2014, accessed on the 27th October, 2014, at 3:40pm.
[549] Solon, (note 543 above)..
[550] _The Serious Crime Bill and Related Material', Equality and Diversity Forum online issue of the 23rd October, 2014, accessed on the 27th October, 2014, at 3:40pm.
[551] *R v Ryan Cleary, Jake Davis, Ryan Akroyd and Mustafa Al-Bassam* (Southwark Crown Court), 16th may, 2013; *R v Christopher Weatherhead, Ashley Rhodes, Peter Gibson, and Jake Burchall*, (Southwark Crown Court), 24th january, 2013, both groups were found to have committed offences in breach of Section 1 and 3 of the CMA, _Computer Misuse Act, 1990 Cases', accessed at http://www.computerevidence.co.uk/Cases/CMA.htm, on the 29th August, 2014, at 1:01pm.

taken place in London and so English courts would not have had jurisdiction to try the offender[552].

However, the Computer Misuse Act is empowered with jurisdiction to try all CMA defined offences, provided that there exists "at least one significant link with the domestic jurisdiction" (England and Wales) in the circumstances of the case[553]. In essence, the CMA alters the previous position, by making it an offence to use a computer to commit a crime in another country and to commit a crime in the UK from a computer in another country[554]. For instance, in the case of *R v Waddon*[555], the English Court of Appeal held that the content of American websites could come under British jurisdiction when downloaded in the United Kingdom[556].

This is an important measure because it reflects a legislation made with a good grasp of the intricacies of the e-commerce trade. This reflects a progressively enlightened trend, as e-commerce can only thrive in the wake of relevant Legislation which is sensitive to the dynamic nature of this field of law, which is subject to change at the invention of a new technology. The CMA is said to be drafted broadly and generally with the aim being its continued relevance to accommodate future technological advancements as well as to prevent it from being rendered inapplicable at the advent of new technology[557]. For instance, the CMA purposely did not provide a definition for the word _œomputer', due to the possibility of the act becoming outdated by a narrow definition, in view of the rapidity with which technology develops[558].

However, a recognised shortfall in the application of CMA, which also applies in the case of most other e-commerce Legislations, as well as the South African Legislation, is the issue of

---

[552] _Computer Misuse Act', accessed at http://www.lawteacher.net/criminal-law/essays/computer-misuse-act.php, on the 29th August, 2014, at 12:50pm.
[553] The Computer Misuse Act, 1990, legal Guidance, A to C accessed at http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/, on the 29th August, 2014 at 12:01pm.
[554] _Computer Misuse Act', accessed at http://www.lawteacher.net/criminal-law/essays/computer-misuse-act.php, on the 29th August, 2014, at 12:50pm.
[555] (2000) All ER (D) 502 (CA).
[556]The Computer Misuse Act, 1990, legal Guidance, A to C accessed at http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/, on the 29th August, 2014 at 12:01pm. See also *R v Perrin* (2002) 4 Archbold News 2, CA.
[557] The Computer Misuse Act, 1990, legal Guidance, A to C accessed at http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/, on the 29th August, 2014 at 12:01pm.
[558] The Computer Misuse Act, 1990, legal Guidance, A to C accessed at http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/, on the 29th August, 2014 at 12:01pm. Tablets and Cellular phones are used to send e-mails.

whether judges possess specialized knowledge of computer technology systems and the possibility of them making inappropriate interpretations of the law, based on this deficit of knowledge[559]. This problem arose during the case of *R v Cropp*[560] where the judge acquitted the defendant as he felt that an offence was only committed if one computer is used to obtain material stored on another computer[561].

This leads to an inquiry of the effectiveness of this legislation (the CMA), as a suitable deterrent to offenders. In reality, only so much can be achieved by legislation, as the virtual nature of the internet makes it easy for crimes to be committed under the veil of anonymity, with relative ease. The CMA is a viable instrument for checking unauthorized access to computer systems, although it may not be the perfect instrument, it is a step in the right direction. At this point the recommendations for the further development of a robust e-commerce Legal framework for the African countries under review are pertinent.

5.3. Recommendations.

It is suggested that a Cyber Appellate Tribunal may be set up / adopted across the board Nations under review, to cater for e-commerce matters[562], which will consist of well trained personnel, who are kept abreast of the developments and trends in the sphere of e-commerce law. In addition, this would significantly reduce the burden on the courts in the countries under review and serve the function of giving e-commerce matters priority[563]. This tribunal is proposed to play the role of ameliorating the problem of lack of specialized knowledge by judges of e-commerce matters, as discussed in the previous chapter.

In the case of South Africa, the tribunal is anticipated to be able to solve the problem of non-designation of a specific court(s) vested with jurisdiction to entertain causes of action which arose abroad, in terms of Section 90 of the ECTA, as discussed above. While in the case of the

---

[559] _Computer Misuse Act', accessed at http://www.lawteacher.net/criminal-law/essays/computer-misuse-act.php, on the 29th August, 2014, at 12:50pm.
[560] Snaresbrook Crown Court 05/07/1991 [1991] 7 CLSR 168, [1991] CL&P July/August 270 Computer Weekly 11 July 1992.
[561] _Computer Misuse Act', accessed at http://www.lawteacher.net/criminal-law/essays/computer-misuse-act.php, on the 29th August, 2014, at 12:50pm.
[562] F, Cassim, _Formulating Specialised Legislation to Address the growing spectre of Cybercrime: A Comparative Study' P.E.R, vol. 12, no. 4, 2009, accessed at http://www.nwu.ac.za/files/images/2009x12x4_Cassim_art.pdf on the 14th January, 2014, at 06:34pm, 36-79, at 65.
[563] Ibid.

United Kingdom, it is expected to ensure more appropriate pronouncements and judgments on e-commerce related matters[564]. Furthermore, it is also expected to effectively forestall the revenue losses[565] of the governments in the countries under review[566].

Moreover, it is also submitted that upon the passage of Nigeria's (Cyber-crime) Bill into Law[567], the relevant commission contemplated in the Bill to be charged with the role of monitoring and regulating e-commerce activities in the republic, should be set up[568]. In addition, proper arrangements should be made for the constant training of its personnel, to keep them updated of the current trends in the ICT world, and a tribunal set up[569]. This approach is aimed at keeping each country's style of handling e-commerce matters or churning out policies on e-commerce issues germane, sensitive to its peculiarities and on the whole, aid the efficiency of the Legal regime.

Furthermore, a lesson may be learnt from the UK's initiative of introducing a collaborative initiative involving the police, members of the private sector and academics jointly working together to stamp out cyber-crimes[570]. This is an ingenious and commendable step in the sense that various stakeholders in the economy are brought together from various walks to contribute a significant measure of information, based on their knowledge and experiences to make practical propositions on how to address the growing menace of cyber-crimes[571]. This has the potential of significantly downplaying the shortfalls of the ICT technology, while making room

[564] In view of the tendency of Judges to make inappropriate rulings, based on wrong notions and incorrect knowledge of computer technology systems and operations.
[565] A, Wakefields, _Cybercrime National Crisis Costing SA R1B a Year', Mail and Guardian issue of 23rd October, 2013, accessed at http://mg.co.za/article/2013-10-23-cybercrime-costing-sa-r1b-a-year, on the 21st March, 2014 at 9:33pm; P, Coetzer, _CyberCrime Escalates in South Africa, Losing the Global Battle against Online Fraud', April 19, 2013 issue of the Leadership Magazine, accessed at http://www.leadershiponline.co.za/articles/cyber-crime-escalates-in-south-africa-6053.html, on the 21st January, 2014, at 04:27pm.
[566] The United Kingdom is reported to experience losses in the region of £70 billion per annum, while South Africa loses an estimate of R1 billion per annum to cyber-crimes. As discussed in chapter 2 above. Ibid.
[567] By way of the awaited Presidential Assent.
[568] In terms of Part V of the Cybercrime Bill. See appendix B below, for specific provisions of the Cybercrime Bill.
[569] As suggested in the first paragraph of the recommendations above.
[570] F, Cassim, _Formulating Specific Legislation to Address the growing spectre of Cybercrime: A Comparative Study' P.E.R, vol. 12, no. 4, 2009, accessed at http://www.nwu.ac.za/files/images/2009x12x4_Cassim_art.pdf on the 14th January, 2014, at 06:34pm, 36-79, at 48.
[571] Ibid.

for its virtues to spring forth. This approach may be adopted in overseeing e-commerce activities in African countries generally, rather than the sphere of cyber-crimes only.

In addition the coalition of select members of the private sector, the police and academics may even be granted audience to make recommendations to the Tribunal on a prescribed basis (this may be annually, bi-annually or quarterly) on current trends in the field of e-commerce and/or play an advisory role in certain decisions of the council. This is hoped to ensure that the policies and / or decisions made by the tribunal are relevant for their purposes, as ratified by a body of pertinent stakeholders.

Furthermore, African developing countries may also glean a thing or two, from some of the International Legal instruments regulating e-commerce, discussed in chapter three above. For Instance, the UNCID rules are instructive, which go a notch higher the MLEC and MLES, which most e-commerce legislations are modeled against, by not only stipulating that a high standard is employed in ensuring the security of data messages, it also sets down rules to the effect that where it forms part of the contract between the sender and recipient that the recipient acknowledges receipt of a data message, the recipient is precluded from the use of such data message until such acknowledgement is sent to the sender[572].

In addition, the GUIDEC rules are equally useful, as they tend to complement the model laws, by legislating upon certain grey areas which the model laws failed to touch on. This can have an overall effect of producing a well-rounded e-commerce Legislation for African countries. For instance, it stipulates particular message authentication procedures to be adopted. It provides that a message be certified and that a recipient may rely on the certificate as accurately representing the facts set forth in it, provided that he has no notice that the certifier failed to satisfy a material aspect of a message authentication process[573].

From the above discourse, if there is any lesson that has been learnt from the evolvement of the CMI of the UK and Nigeria, prior to specific e-commerce legislation, it is that the nature of cyber-crime evolves with changing technology. It is suggested that e-commerce legislations be

[572] Article 8(a) UNCID.
[573] Guidec II, X – Certification, accessed at www.iccwbo.org/Advocacy-codes-and-Rules/Document-centre/2001/GUIDEC-General-Usage-for-International-Digitally-Ensured-Commerce-%28Version-11%29-01/10/2001/ on 13th May, 2014 at 12:29pm.

couched in the form of a living document, just like the GUIDEC, discussed above. The aim is to ensure the relevance of the substantive legislation, to accommodate technological changes and new horizons of cyber-crime.

Not forgetting implementation, the individual governments of African countries should also endeavor to develop specialized know how on the nature of cyber-crimes, by way of sponsorship of individuals willing to study in this area, to serve an incentive and in the long run, create a formidable pool of e-commerce technology savvy personnel.

Furthermore, computer ethics education may also be taught in schools[574] to reduce the prevalence of cyber-crime, and to discourage the practice of the abuse of internet transactions, with reliance on the veil of anonymity. These recommendations are anticipated to answer the queries as regards lack of specialized knowledge of computer operations by judges making decisions on e-commerce matters and make for an effective implementation regime, in line with the conclusion reached in the previous chapter.

5.4 Conclusion.

This thesis set out to investigate the root cause of the problems African countries face in terms of their operative e-commerce Legal frameworks. The study revealed that certain African countries had domesticated Legislation in relation to e-commerce[575], while some other were yet to have defined e-commerce Legislation[576]. However, both countries with specific e-commerce Legislation and those without such legislation grappled with somewhat similar problems[577], but on rather different scales[578]. The root cause of the glitches was found to lie in the

[574] F, Cassim, _Formulating Specific Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study' P.E.R, vol. 12, no. 4, 2009, accessed at http://www.nwu.ac.za/files/images/2009x12x4_Cassim_art.pdf on the 14th January, 2014, at 06:34pm, 36-79, 68. <http://www.puk.ac.za/opencms/export/PUK/html/fakulteite/regte/per/issuepages/2009Volume12no4/2009x12x4_Cassim_art.pdf>, accessed 14th January, 2014, 6:50pm.

[575] Such as South Africa.

[576] Such as Nigeria.

[577] Cybercrimes, Revenue Losses.

[578] Nigeria's situation is obviously worse off, in comparison to the other countries under review, as its laws do not specifically outlaw several areas of misconduct, such as hacking, spamming, denial of service attacks, amongst other cyber-crimes and they go on unchecked, costing the economy several millions or even billions of Naira. This represents the situation of countries without e-commerce Legislation. While in a country like South Africa which outrightly outlaws similar areas of misconduct, successfully prosecutes a number of them, but is unable to clamp down on each and every one of these activities. Losses result, but efforts are ongoing to curb the excesses.

implementation mechanism adopted by countries with specific legislation[579]. In essence, it has been gleaned from the discourse above that implementation of a legal regime alone is not enough, but an effective implementation regime must be in place, in order to make for efficiency of the existing legal regime.

Moreover, the concept of electronic commerce has been explored, and it has been found to encompass all forms of business transactions in which parties interact electronically, rather than by direct physical contact[580]. In addition, the national and international legal frameworks governing e-commerce, as well as the benefits derived from e-commerce have been explored at some length[581]. Furthermore, the effectiveness of each of the applicable laws has been examined in view of the economic reality in each of the countries under review, which led to apposite recommendations.

In view of the above continuum, it is evident that Nigeria's current legal regime is highly ineffective in regulating e-commerce activities in the republic. While, South Africa, on the other hand, presents an encouraging case study in the sense that its legislation (the ECTA), qualifies as a viable tool for the regulation of e-commerce activities in the republic, as has been revealed through case law. However, the most critiqued aspect of this legislation is the fact that the penalties set were too minute, and were unlikely to effectively instill compliance to its provisions[582]. It is interesting to note that this area has been addressed by the *ECTA Amendment Bill, 2012*, which sets stiffer penalties than were previously applicable.

Furthermore, the United Kingdom presents an equally interesting case study as it also amended its existing law (the CMA) a number of times to bring it in line with current trends. This is reflective of the Legislature's attempt at keeping pace with the technology, in view of the dynamic nature of technology, which has the ability to render legislation in this field outdated. This approach is lauded and it is hoped that the African countries under review take the cue from the United Kingdom in this light.

---

[579] As is the case in South Africa, as discussed in the first part of this chapter.
[580] J Lourens, _Electronic Commerce, The Law and its Consequences' <http://butterworths.ukzn.ac.za/nxt/gateway.dll/zkfaa/bsxha/73dba/f4dba/6liba/pzeua> pg 1, accessed 1st March, 2013, 04:50pm.
[581] In chapter two, above.
[582] Cassim (note 569 above) 59.

In conclusion, it is hereby suggested that Law enforcement agents as well as members of the legislature, who are charged with the duty of enforcing and making amendments to this legislation respectively, need to be enlightened of and kept abreast of developments in the area of e-commerce as relates to their roles, in order to ensure the further development of a more secure legal framework for the flourishing of e-commerce.

BIBLIOGRAPHY.

1.1 PRIMARY SOURCES

- ***CONVENTIONS.***
  - The Uncitral {United Nations' Commission on International Trade Law} Model Law on Electronic Commerce 1996 [MLEC].
  - The Uncitral {United Nations' Commission on International Trade Law} Model Law on Electronic Signatures 2001 [MLES].
  - The United Nations' Convention on the Use of Electronic Communications in International Contracts 2005 (UNECIC).
- ***RULE GOVERNING ELECTRONIC LETTERS OF CREDIT.***
  - The Supplement To The Uniform Customs And Practice For Documentary Credits For Electronic Presentation (Eucp) Version 1.1
- ***SOUTH AFRICAN STATUTES:***
  - The Electronic Communications and Transactions Act (ECTA) (25 of 2002).
  - Natal Law 12 of 1884; Act 68 of 1957; Act 71 of 1969; Act 68 of 1981.
  - The Constitution of the Republic of South Africa, 1996.
  - Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002
- ***NIGERIAN STATUTES:***
  - The Evidence (Amendment) Act, 2011.
  - The Interpretation Act, Laws of the Federation of Nigeria, 2004.
  - Advance Fee Fraud and other Fraud Related Offences Act 2006.
  - The Constitution of the Federal Republic of Nigeria, 1999.
- ***NIGERIAN DRAFT BILL:***

  The Bill for an Act to Provide for the Prohibition, Prevention, Detection, Response and Prosecution of Cyber Crimes and Other Related Matters 2013 (The Cyber rime Bill 2013).

1.2 SECONDARY SOURCES

- ***TEXTBOOKS.***

1. Carr I & Kidner, R, Statutes and Conventions on International Trade Law 4th ed. (2003).
2. Carr, I, International Trade Law 4th ed. (2010), part II, Cavendish Publishing Limited.
3. Chaffey D, E-Business and E-Commerce Management 2nd ed. (Prentice Hall Harlow 2003), 16.

4. Christie RH, ‗The Law of Contract in South Africa' (2006) 5th ed. LexisNexis Butterworths.

5. Christie, RH ‗Law of Contract in South Africa', (1996) 3rd ed.

6. Davis O –Contract Formation on the Internet: Shattering a Few Myths" in Edwards L and Waelde c (ed) Law and the internet, Hart Publishing Oxford (1997), 100.
7. Gringas C and Nabarro N, ‗*The Laws of the Internet'* (Butterworths London 1977).

8. Hofman J, Johnston D, Handa S & Morgan C, Cyberlaw C: A Guide for South Africans Doing Business Online, Cape Town: Ampersand. Dunlop (2005)

9. Kalakota R & Whinston, A, *Electronic Commerce A Manager's Guide* 3rd ed. (Addison Wesley Reading 1997), 69.

10. Reed C: Internet Law: Text and Materials, Butterworths, London, Edinburg, Dublin (2000)

11. Siebel TM & House P, Cyber Rules - Strategies for Excelling at E-business, Currency and Doubleday, May 1999. New York.

12. Singleton S &Halberstam S: ‗Business, the Internet and the Law', 1999, Trolley, London.

13. Yee Fen Lim: Cyberspace Law Commentaries and Materials, Oxford University Press, (2003)

1.3 CASES.

14. Anyaebosi v. R. T Briscoe Nigeria Ltd [1987] 3 Nigeria Weekly Law Reports 84 (part 59).
15. Anyaebosi v. R. T Briscoe Nigeria Ltd[1987] 3 Nigeria Weekly Law Reports 84 (part 59).
16. Douvenga R v. {District Court of the Northern Transvaal, Pretoria, case no 111/150/2003,19 August 2003(unreported case)}.
17. Georgia Dept. of Transportation v. Norris 1997. 474 S.E.2d 216 (Ga. App. 1996).
18. Goldblatt v. Fremantle (1920) AD 123, 128.
19. Jafta v. Ezemvelo KZN Wildlife(D204/07) [2008] ZALC 84; [2008] 10 BLLR 954 (LC); (2009) 30 ILJ 131 (LC) (1 July 2008).
20. Mashiyi S v and Another2002 2 SACR 387.
21. Ndiki S v. and others 2008 SACR 2 258.
22. Nuba Commercial Farms Ltd v NAL Merchant Bank Ltd & anor [2001] 16 NWLR 510 (part 740),

23. Nuba Commercial Farms Ltd v NAL Merchant Bank Ltd & anor[2001] 16 NWLR 510 (part 740).
24. Reid Bros (SA) Ltd v Fischer Bearings Co. Ltd (1943) AD 232 241.
25. Scherierhout v. Minister of Justice (1926) AD 99 109.
26. Uganda v Garuhanga and Mugerwa (CR 17 of 2004 Bugand Road Court).

1.4 JOURNAL ARTICLE

1. Akintola KG, Akinyede RO & Agbonifo CO: –Appraising Nigeria Readiness for E-Commerce towards achieving vision 20:2020" Nov. 2011 www.arpapress.com/Volumes/Vol9Issue2/IJRRAS_9_2_18.pdf

2. Akomolede TI, _Contemporary Legal Issues in Electronic Commerce in Nigeria' (2008) Potchefstroom Electronic Law Journal 1, 8.
3. Aldrich M,. *'The Inventor's Story, Aldrich Archive'* (University of Brighton, 2008) <http://www.aldricharchive.com/inventors_story.html> (accessed 21st November 2013).
4. Ayo C. K, Adebiyi A. A.; I.T. Fatudimu, and U. O. Ekong , _A Framework for e-Commerce Implementation:

5. Bamodu, 'Information Communications Technology and E-Commerce: Challenges and Opportunities for the Nigerian Legal System and the Judiciary', (2002) 2 The Journal of Information, Law and Technology (JILT). <http://www2.warwick.ac.uk/fac/soc/law2/elj/jilt/2004_2/bamodu/>.
6. Bellare M & Rogaway P: _Message Authentication', ch.7, pg. 1, accessed at http://cseweb.ucsd.edu/~mihir/cse207/w-mac.pdf, on the 21st of May, 2014 at 6:49pm.
7. Bezuidenhout, PS & Glout, JD, _Identifying the risks in e-commerce payment for use by the IS Auditor', South African Journal of Auditing and Accountability Research, vol 4: 2003 (21-35) at pg 21.
8. Cassim F, _Formulating Specific Legislation to Address the growing spectre of Cybercrime: A Comparative Study' P.E.R, vol. 12, no. 4, 2009, <http://www.puk.ac.za/opencms/export/PUK/html/fakulteite/regte/per/issuepages/2009Volume12no4/2009x12x4_Cassim_art.pdf>, accessed 14th January, 2014, 6:50pm.
9. Cassim, F _Addressing the growing spectre of cyber crime in Africa : evaluating measures adopted by South Africa and other regional role players' , (2011) Comparative and International Law Journal of Southern Africa, Vol 44, Issue 1, Mar Pages: 123-138 , p. 127.
10. Dagada R, Eloff MM & Venter LM _Too Many Laws but very little progress Is South Africa's Highly acclaimed Information Security Legislation Redundant?' available at http://uir.unisa.ac.za/bitstream/handle/10500/2660/dagada.pdf?sequence=1 , accessed on 15 July 2013.
11. European Commission, _A European Initiative in Electronic Commerce', Communication from the Commission

12. Ewelukwa N., _Is Africa Ready for Electronic Commerce? A Critical Appraisal of the Legal Framework for ECommerce in Africa' <http;//www.acicol.com/temp/Dr N.pdf >
13. Gakuru M, Winters K and Stepman F, _Inventory and Innovative Farmer Advisory Services Using ICTs', is instructive, being an initiative of the Forum for Agricultural Research in Africa, 2009, last accessed at http://www.fara-africa.org/media/uploads/File/NSF2/RAILS/Innovative_Farmer_Advisory_Systems.pdf , on the 5th September 2014 at 2:38pm.
14. Gib A _E-Commerce Development' http://www.articlesnatch.com/Article/A-Brief-History-Of-E-commerce/634686#.Uo4nxScgh9s (accessed 21st November 2013).
15. Gonzalez L., _The Theory of Comparative Advantage' (2004) <http://www.freerepublic.com/focus/f-news/1101717/posts> Posted on Saturday, March 20, 2004 5:54:53 AM.
16. Goodman MD & Brenner S _The emerging consensus on criminal conduct in cyberspace' 2002 *International Journal of Law and Information Technology*139–223 at 142, 146–150.
17. Hunton P, _The growing Phenomenom of Crime and the Internet: A Cybercrime analysis and execution model', 2009, Computer Law and Security Review, 528-535, at 530.
18. Kamssu AJ, Siekpe JS & Ellzy JA, _Shortœomings to Globalisation: Using Internet Technology and Electronic Commerce in Developing Countries' (2004) 38 The Journal of Developing Areas.
19. Le Roux F, _E-Commerce: The Legal Framework' <http://butterworths.ukzn.ac.za/nxt/gateway.dll/zkfaa/bsxha/azjba/izjba/gwmba/pydua> .
20. Lourens J, _Electronic Commerce, The Law and its Consequences' <http://butterworths.ukzn.ac.za/nxt/gateway.dll/zkfaa/bsxha/73dba/f4dba/6liba/pzeua
21. MacEwan N, _The Computer Misuse Act 1990: Lessons from its past and Predictions for its future' (2008) Criminal Law Review, pg 1-9 at 5, accessed at http://usir.salford.ac.uk/15815/7/MacEwan_Crim_LR.pdf, on the 16th August, 2014 at 10:36am.
22. Mahlaka R –Online Shopping: Is SA ready for it?" Moneyweb online article accessed at http://www.moneyweb.co.za/moneyweb-south-africa/online-shopping-is-sa-ready-for-it, on the 17th June, 2014 at 04:58pm.
23. Nigeria a Case Study' (2008), Journal of Internet Banking and Commerce, August 2008, vol. 13, no.2, accessed at http://www.arraydev.com/commerce/jibc/2008-08/ayo.pdf, on the 6th September, 2014 at 5:28pm.
24. Oduntan O A, _Taxation of Electronic Commerce: Prospects and challenges for Nigeria' 2010, electronic copy available at: http://ssrn.com/abstract=1697998, pg 14

25. Oyewunmi A., _The ICT Revolution and Commercial Sectors in Nigeria: Impacts and Legal Interventions‘ (2012) 5, British journal of Arts and Social Sciences <*http://www.bjournal.co.uk/BJASS.aspx*>.
26. Oyewunmi AO : –The ICT Revolution and Commercial Sectors in Nigeria: Impacts and Legal Interventions", British Journal of Arts and Social Sciences, vol. 5, No. 2 2012,ISSN 2046-9578, accessed at http://www.bjournal.co.uk/paper/bjass_5_2/bjass_05_02_08.pdf, on the 4th March, 2013 at 06:12pm.
27. Regions - Brussels, 16th April 1997, COM(97) 157 final.
28. Roberts M,, _Ecommerce Development ‘ http://www.articlesnatch.com/Article/Ecommerce-Development/2635543#.Uo4nlScgh9s accessed 28th November, 2013, 05:16pm.
29. Rodriguez T, –Applicable Law and Jurisdiction in Electronic Contracts I" < http://www.emarketservices.com/clubs/ems/prod/E-Business%20Issue%20-Applicable%20law%201(1).pdf>, e-Business issue, December 2010, accessed on the 5th December, 2013, at 12:14pm, 2.
30. Schonfeld E, –Forrester Forecast: Online Retail sales will grow to $250 billion by 2014", techcrunch.com 8th March 2010 issue, < http://techcrunch.com/2010/03/08/forrester-forecast-online-retail-sales-will-grow-to-250-billion-by-2014/ > , accessed 11th December 2013, 05:13pm.
31. Siebel, T.M. & House, P. 1999. _Cyber Rules - Strategies for Excelling at E-business‘. *Currency and Doubleday*. May 1999. New York. p50.
32. Smedinghoff TJ & RH Bro, _Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce‘, 17 J. Marshall J Computer and Info. L. 723, (1999) at 730, accessed at http://repository.jmls.edu/cgi/viewcontent.cgi?article=1260&context=jitpl on 25th March, 2014.
33. Snail S –Jurisdiction in Electronic Trans-Border Contracts" Kwazulu-Natal Law Society <https://www.lawsoc.co.za/default.asp?sl=&id=1888>, accessed on the 5th December, 2013 at 12:50pm.
34. to the Council, The European Parliament, The Economic and Social Committee and the Committee of the
35. Tushabe F & Baryamureeba V _Cyber Crime in Uganda: Myth or Reality?‘ Proceedings of World Academy of Science, Engineering and Technology, Vol. 8, p.68, 8th October, 2005, ISSN 1307-6884.
36. Tushabe F & Baryamureeba V _Cyber Crime in Uganda: Myth or Reality?‘ Proceedings of World Academy of Science, Engineering and Technology, Vol. 8, p.68, 8th October, 2005, ISSN 1307-6884.

1.4 INTERNET SOURCES

- ***WEBSITES.***

1. Bakibinga D _Cyber crime in Uganda' available at: http://www.dpp.go.ug/perspectives
2. Counseil Europeen des Federations l'Industrie Chimique; www.cefic.be.
3. Cyber Crimes Watch, 11th September 2011 < www.cybercrimeswatch.com/cyber-crime/cyber-crime-statistics.html > accessed on the 16th of May, 2013.
4. Kganyago, K, _How Serious is Internet related crime in South Africa' <http://kganyago.org/2012/11/05/how-serious-is-internet-related-crime-in-south-africa/>, accessed on the 5th of November, 2013, 4:40am
5. Ecommerce definition and types', accessed 22nd November, 2013, 02:37pm. http://www.digitsmith.com/ecommerce-definition.html

6. Ecommerce Models' http://www.eservglobal.com/uploads/files/index.pdf, accessed 2nd December, 2013, 03:16pm.
7. E-commerce webhosting guide < http://www.ecommerce-web-hosting-guide.com/ecommerce-business-models.html >, accessed 29th November, 2013, 8:51am.https://www.fnb.co.za/downloads/PAYPAL-quick-guide-FNB.pdf>

8. Edibasics website, _What is Edi? ' accessed at http://www.edibasics.com/what-is-edi/, on the 13th of May, 2014, at 02:10pm.
9. FORMATION OF CONTRACTS:http://www.out-law.com/page-396

10. General Usage for International Digitally Ensured Commerce' accessed at http://ecommerce.hostip.info/pages/477/General-Usage-International-Digitally-Ensured-Commerce-GUIDEC.html on the 16th of May, 2014 at 07:35pm.
11. Gov. UK Press Release, _Business Leaders urged to step up response to Cyber Threats', 5th September, 2012,<https://www.gov.uk/government/news/business-leaders-urged-to-step-up-response-to-cyber-threats>, accessed on the 14th of January, 2014, 1:17pm.
12. Gov. UK Press Release, _Business Leaders urged to step up response to Cyber Threats', 5th September, 2012,<https://www.gov.uk/government/news/business-leaders-urged-to-step-up-response-to-cyber-threats>, accessed on the 14th of January, 2014, 1:17pm.

13. GUIDEC II, accessed at http://cryptome.org/jya/guidec2.htm, on the 17th, May, 2014 at 12:35pm.
14. http://en.wikipedia.org/wiki/Electronic_funds_transfer.

15. http://searchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies, on the 5th September, 2014 at 2:15pm.
16. http://www.out-law.com/page-396, accessed on the 28th of March, 2013, at 08:45am.
17. http://www.techterms.com/definition/edi, on the 13th of May, 2014, at 02:28pm. http://www.tutorialspoint.com/e_commerce/e_commerce_business_models.htm, accessed 28th November, 2013, 3:47pm.

18. http://www.uncitral.org/pdf/english/congress/Ribadu_Ibrahim.pdf> accessed on 4th of March, 2013, at 03:06pm.
19. http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html>, accessed on the 8th of March, 2013, at 03:59pm.
20. http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html> accessed on the 15th of July, 2013.
21. http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html
22. http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html
23. http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/1996Model.html> accessed on the 8th of March, 2013 at 03:59pm.
24. http://www.wisegeek.com/what-was-the-purpose-of-the-computer-misuse-act.htm, on the 28th August, 2014, at 1:24pm.
25. http://www-01.ibm.com/software/commerce/b2b/edi/, on the 13th of May, 2014, at 02:28pm.
26. https://www.paypal.com/webapps/mpp/buy.
27. Internet World Stats <http://www.internetworldstats.com/stats.htm> accessed 4th April, 2013.
28. Investing Answers, accessed at http://www.investinganswers.com/financial-dictionary/personal-finance/electronic-funds-transfer-eft-2328, on 19 November, 2014 12:45pm.
29. IT News Africa, 16th of May, 2013 < www.itnewsafrica.com/2013/01/south-african-cybercrimw-set-to-soar-in-2013/ > accessed on the 16th of May, 2013.
30. Legislation and its Impact: The Impact of the Computer Misuse Act', accessed at http://www.sqa.org.uk/e-learning/ProfIssues02CD/page_08.htm, on the 16th August, 2014, at 10:37am.
31. National Barcode Website, accessed at http://www.nationalbarcode.com/articles/what-is-a-barcode.html, on the 19 November, 2014, 01:05pm.
32. Nickov A, _eCommerce Business Models and Concepts', http://www2.sta.uwi.edu/~anikov/comp6350/lectures/02-ECS-lect-eCommerce-business-models-concepts.pdf, accessed on 5th December 2013 at 10:54am, pg 8.
33. Organisation for Data Exchange by Teletransmission in Europe; www.odette.org.
34. Pacini C, Andrews C & Hillison W, _Legal Issues in Online Contracting: To agree or not to Agree' http://dx.doi.org/10.1016/S0007-6813(02)80009-X, accessed on the 25th April, 2013, at 11:39am, 1.
35. PC Tools by Symantec, 14th October, 2010, <www.pctools.com/security-news/african-cybercrime/ > accessed on the 16th of May, 2013.
36. REGULATING NIGERIAN E-COMMERCE: http://www.iflr.com/Article/3020851/Regulating-Nigerian-e-commerce.html

37. Security Service, M15, _How is M15 tackling the Security Threat‘ < https://www.mi5.gov.uk/home/the-threats/cyber/how-is-mi5-tackling-the-cyber-threat.html >, accessed on the 14th of January, 2014, 3:37pm.
38. The Business Dictionary Website, accessed http://www.businessdictionary.com/definition/electronic-imaging.html, on the 19 November, 2014, 01:15pm.
39. The International Chamber of Commerce website, accessed at http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2001/GUIDEC-General-Usage-for-International-Digitally-Ensured-Commerce-(Version-II)-01/10/2001/, on the 13th May, 2014 at 12:29pm.
40. The Law Teacher, < http://www.lawteacher.net/contract-law/lecture-notes/agreement-lecture.php >.
41. UNCITRAL MODEL LAW ON ELECTRONIC COMMUNICATIONS 1996 TEXTS: http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/1996Model.html
42. UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES 2001TEXTS:
43. UNITED NATIONS CONVENTION ON THE USE OF ELECTRONIC COMMUNICATIONS IN INTERNATIONAL CONTRACTS 2005 TEXTS:
44. United Nations Economic Commission for Europe website, accessed at http://www.unece.org/tradewelcome/areas-of-work/un-centre-for-trade-facilitation-and-e-business-uncefact/outputs/standards/unedifact/tradeedifactrules/part-2-uniform-rules-of-conduct-for-interchange-of-trade-data-by-teletransmission-uncid/part-2-uncid-chapter-4-interchange-agreement.html, on the 13th of May, 2014, at 05:05pm.
45. Van der Merwe, M & Janse van Vuuren, J, _Internet Contracts‘, pg. 156, accessed at http://www.legalnet.co.za/cyberlaw/cybertext/chapter6.htm, 12th December, 2013 at 6:27pm.
46. www.oecd.org/eco/outlook/2087433.pdf.

1.5 NEWSPAPERS

1. Akintola KG, Akinyede RO & Agbonifo CO: –Appraising Nigeria Readiness for E-Commerce towards achieving vision 20:2020” Nov. 2011 www.arpapress.com/Volumes/Vol9Issue2/IJRRAS_9_2_18.pdf p. 9.
2. Anonymous _Waiter jailed for credit card fraud‘ available at: http://www/news24.com/SouthAfrica/News (accessed on 19 October 2010).
3. Bradley T, _Cybercrime siphons $3 billion in E-Commerce Revenue‘, Salted Hash – Top Security News, 14th January, 2014, <http://blogs.csoonline.com/malwarecybercrime/2753/cybercrime-siphons-3-billion-e-commerce-revenue>, accessed on 14th January, 2014, 12:47pm. _UK bans denial of Service Attacks‘, The Register online issue of the 12th of November, 2006. Accessed at http://www.theregister.co.uk/2006/11/12/uk_bans_denial_of_service_attacks/, on the 27th August, 2014, at 1:49pm.
4. Coetzer P, –CyberCrime Escalates in South Africa, Losing the Global Battle against Online Fraud”, April 19, 2013 issue of the Leadership Magazine, accessed at

http://www.leadershiponline.co.za/articles/cyber-crime-escalates-in-south-africa-6053.html, on the 21st January, 2014, at 04:27pm.

5. Elebeke E _Why cybercrime thrives in Nigeria by Ewelukwa' 13th April, 2011, Vanguard Newspapers < www.vanguardngr.com/2011/04/why-cyber-crime-thrives -in-nigeria-by-ewelukwa/ > accessed on the 16th of May, 2013.
6. Lisandro A. Allende & Mariana A. Miglino, Internet Law - International Electronic Contracting: The UN Contribution, Ibls Internet Law - News Portal, Mar. 6, 2007, http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1610 (last visited Mar. 6, 2007).
7. Ryan E, *Sunday Times* _Ugly world of criminals who go phishing' 27 June 2010 8.
8. Wakefields A : Cybercrime National Crisis Costing SA R1B a Year, Mail and Guardian issue of 23rd October, 2013, accessed at http://mg.co.za/article/2013-10-23-cybercrime-costing-sa-r1b-a-year, on the 21st March, 2014 at 9:33pm.

APPENDIX A (SOUTH AFRICAN LEGISLATION)-

ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002.

"data message" means data generated, sent, received or stored by electronic means and includes

(a) voice, where the voice is used in an automated transaction; and

(b) a stored record;

"electronic communication" means a communication by means of data messages;

"electronic signature" means data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature;

"e-mail" means electronic mail, a data message used or intended to be used as a mail message between the originator and addressee in an electronic communication;

"Internet" means the interconnected system of networks that connects computers around the world using the TCP/IP and includes future versions thereof,
"personal information" means information about an identifiable individual, including, but not limited to

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

(c) any identifying number, symbol, or other particular assigned to the individual;

(d) the address, fingerprints or blood type of the individual;

(e) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;

(f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the individual;

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but excludes information about an individual who has been dead for more than 20 years;

CHAPTER III -FACILITATING ELECTRONIC TRANSACTIONS

Part 1

Legal requirements for data messages

11. Legal recognition of data messages

(1) Information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message.

(2) Information is not without legal force and effect merely on the grounds that it is not contained in the data message purporting to give rise to such legal force and effect, but is merely referred to in such data message.

(3) Information incorporated into an agreement and that is not in the public domain is regarded as having been incorporated into a data message if such information is -

(a) referred to in a way in which a reasonable person would have noticed the reference thereto and incorporation thereof; and

(b) accessible in a form in which it may be read, stored and retrieved by the other party, whether electronically or as a computer printout as long as such information is reasonably capable of being reduced to electronic form by the party incorporating it.

12. Writing

A requirement in law that a document or information must be in writing is met if the document or information is -

(a) in the form of a data message; and

(b) accessible in a manner usable for subsequent reference.

13. Signature

(1) Where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature is used.

(2) Subject to subsection (1), an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form.

(3) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if

(a) a method is used to identify the person and to indicate the person‘s approval of the information communicated; and

(b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.

(4) Where an advanced electronic signature has been used, such signature is regarded as being a valid electronic signature and to have been applied properly, unless the contrary is proved.

(5) Where an electronic signature is not required by the parties to an electronic transaction, an expression of intent or other statement is not without legal force and effect merely on the grounds that -

(a) it is in the form of a data message; or

(b) it is not evidenced by an electronic signature but is evidenced by other means from which such person‘s intent or other statement can be inferred.

14. Original

(1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if -

(a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and

(b) that information is capable of being displayed or produced to the person to whom it is to be presented.

(2) For the purposes of subsection 1(a), the integrity must be assessed -

(a) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;

(b) in the light of the purpose for which the information was generated; and

(c) having regard to all other relevant circumstances.

15. Admissibility and evidential weight of data messages

(1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence -

(a) on the mere grounds that it is constituted by a data message; or

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message must be given due evidential weight.

(3) In assessing the evidential weight of a data message, regard must be had to -

(a) the reliability of the manner in which the data message was generated, stored or communicated;

(b) the reliability of the manner in which the integrity of the data message was maintained;

(c) the manner in which its originator was identified; and

(d) any other relevant factor.

(4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.

16. Retention

(1) Where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message, if -

(a) the information contained in the data message is accessible so as to be usable for subsequent reference;

(b) the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) the origin and destination of that data message and the date and time it was sent or received can be determined.

(2) The obligation to retain information as contemplated in subsection (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

17. Production of document or information

(1) Subject to section 28, where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of a data message, an electronic form of that document or information, and if -

(a) considering all the relevant circumstances at the time that the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and

(b) at the time the data message was sent, it was reasonable to expect that the information contained therein would be readily accessible so as to be usable for subsequent reference.

(2) For the purposes of subsection (1), the integrity of the information contained in a document is maintained if the information has remained complete and unaltered, except for -

(a) the addition of any endorsement; or

(b) any immaterial change, which arises in the normal course of communication, storage or display

18. Notarisation, acknowledgement and certification

(1) Where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is met if the advanced electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the electronic signature or data message.

(2) Where a law requires or permits a person to provide a certified copy of a document and the document exists in electronic form, that requirement is met if the person provides a print-out certified to be a true reproduction of the document or information.

(3) Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or other physical form, that requirement is met if an electronic copy of the document is certified to be a true copy thereof and the certification is confirmed by the use of an advanced electronic signature.

19. Other requirements

(1) A requirement in a law for multiple copies of a document to be submitted to a single addressee at the same time is satisfied by the submission of a single data message that is capable of being reproduced by that addressee.

(2) An expression in a law, whether used as a noun or verb, including the terms ~~"d~~ocument", ~~"re~~cord", ~~"fi~~le", ~~"s~~ubmit", ~~"lo~~dge", ~~"de~~liver", ~~"i~~ssue", ~~"p~~ublish", ~~"w~~rite in", ~~"p~~rint" or words or expressions of similar effect, must be interpreted so as to include or permit such form, format or action in relation to a data message unless otherwise provided for in this Act.

(3) Where a seal is required by law to be affixed to a document and such law does not prescribe the method or form by which such document may be sealed by electronic means, that requirement is met if the document indicates that it is required to be under seal and it includes the advanced electronic signature of the person by whom it is required to be sealed.

(4) Where any law requires or permits a person to send a document or information by registered or certified post or similar service, that requirement is met if an electronic copy of the document or information is sent to the South African Post Office Limited, is registered by the said Post Office and sent by that Post Office to the electronic address provided by the sender.

20. Automated transactions

In an automated transaction -

(a) an agreement may be formed where an electronic agent performs an action required by law for agreement formation;

(b) an agreement may be formed where all parties to a transaction or either one of them uses an electronic agent;

(c) a party using an electronic agent to form an agreement is, subject to paragraph (d), presumed to be bound by the terms of that agreement irrespective of whether that person reviewed the actions of the electronic agent or the terms of the agreement;

(d) A party interacting with an electronic agent to form an agreement is not bound by the terms of the agreement unless those terms were capable of being reviewed by a natural person representing that party prior to agreement formation.

(e) no agreement is formed where a natural person interacts directly with the electronic agent of another person and has made a material error during the creation of a data message and -

(i) the electronic agent did not provide that person with an opportunity to prevent or correct the error;

(ii) that person notifies the other person of the error as soon as practicable after that person has learned of it;

(iii) that person takes reasonable steps, including steps that conform to the other person‘s instructions to return any performance received, or, if instructed to do so, to destroy that performance; and

(iv) that person has not used or received any material benefit or value from any performance received from the other person.

51. Principles for electronically collecting personal information

(1) A data controller must have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law.

(2) A data controller may not electronically request, collect, collate process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required.

(3) The data controller must disclose in writing to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored.

(4) The data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law.

(5) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected.

(6) A data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or specifically authorised to do so in writing by the data subject.

(7) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed.

(8) The data controller must delete or destroy all personal information which has become obsolete.

(9) A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party.

81. Powers of cyber inspectors

(1) A cyber inspector may -

(a) monitor and inspect any web site or activity on an information system in the public domain and report any unlawful activity to the appropriate authority;

(b) in respect of a cryptography service provider -

(i) investigate the activities of a cryptography service provider in relation to its compliance or non-compliance with the provisions of this Act; and

(ii) issue an order in writing to a cryptography service provider to comply with the provisions of this Act;

(c) in respect of an authentication service provider -

(i) investigate the activities of an authentication service provider in relation to its compliance or non-compliance with the provisions of this Act;

(ii) investigate the activities of an authentication service provider falsely holding itself, its products or services out as having been accredited by the Authority or recognised by the Minister as provided for in Chapter VI;

(iii) issue an order in writing to an authentication service provider to comply with the provisions of this Act; and

(d) in respect of a critical database administrator, perform an audit as provided for in section 57.

(2) Any statutory body, including the South African Police Service, with powers of inspection or search and seizure in terms of any law may apply for assistance from a cyber inspector to assist it in an investigation: Provided that -

(a) the requesting body must apply to the Department for assistance in the prescribed manner; and

(b) the Department may authorise such assistance on certain conditions.

CHAPTER XIII- CYBER CRIME

85. Definition

In this Chapter, unless the context indicates otherwise -

~~"a~~ccess" includes the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data.

86. Unauthorised access to, interception of or interference with data

(1) Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.

(2) A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence.

(3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adepts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence.

(4) A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data of access thereto, is guilty of an offence.

(5) A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence.

87. Computer-related extortion, fraud and forgery

(1) A person who performs or threatens to perform any of the acts described in section 86, for the purpose of obtaining any unlawful proprietary advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions, is guilty an offence.

(2) A person who performs any of the acts described in section 86 for the purpose of obtaining any unlawful advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic, is guilty of an offence.

88. Attempt, and aiding and abetting

(1) A person who attempts to commit any of the offences referred to in sections 86 and 87 is guilty of an offence and is liable on conviction to the penalties set out in section 89(1) or (2), as the case may be.

(2) Any person who aids and abets someone to commit any of the offences referred to in sections 86 and 87 is guilty of an offence and is liable on conviction to the penalties set out in section 89(1) or (2), as the case may be.

89. Penalties

(1) A person convicted of an offence referred to in sections 37(3), 40(2), 58(2), 80(5), 82(2) or 86(1), (2) or (3) is liable to a fine or imprisonment for a period not exceeding 12 months.

(2) A person convicted of an offence referred to in section 86(4) or (5) or section 87 is liable to a fine or imprisonment for a period not exceeding five years.

APPENDIX B (NIGERIAN CYBERCRIME BILL)-

A BILL FOR AN ACT TO PROVIDE FOR THE PROHIBITION, PREVENTION, DETECTION, RESPONSE AND PROSECUTION OF CYBERCRIMES AND FOR OTHER RELATED MATTERS, 2013

ENACTED by the National Assembly of the Federal Republic of Nigeria as follows -

PART I

OBJECT AND APPLICATION

1. Objectives

The objectives of this Act are to –

(a) provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;

(b) ensure the protection of critical national information infrastructure; and

(c) promote cyber-security and the protection of computer systems and networks, electronic communications; data and computer programs, intellectual property and privacy rights.

2. Application

The provisions of this Act shall apply throughout the Federal Republic of Nigeria.

PART II- PROTECTION OF CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

3. Designation of certain computer systems or networks as critical national information infrastructure.

(1) The President may on the recommendation of the National Security Adviser, by Order published in the Federal Gazette, designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria or the economic and social wellbeing of its citizens, as constituting Critical National Information Infrastructure.

(2) The Presidential Order made under subsection (1) of this section may prescribe minimum standards, guidelines, rules or procedure in respect of -

(a) the protection or preservation of critical information infrastructure;

(b) the general management of critical information infrastructure; (d) infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any critical national information infrastructure;

(e) the storage or archiving of data or information regarded critical national information infrastructure;

(f) recovery plans in the event of disaster or loss of the critical national information infrastructure or any part of it; and

(g) any other matter required for the adequate protection, management and control of data and other resources in any critical national information infrastructure.

4. Audit and Inspection of critical national information infrastructure

The Presidential Order made under section 3 of this Act may require the audit and inspection of any Critical National Information Infrastructure, from time to time, to evaluate compliance with the provisions of this Act.

PART III - OFFENCES AND PENALTIES

5. Offences against critical national information infrastructure

(1) Any person who commits any offence punishable under this Act against any critical national information infrastructure, designated pursuant to section 3 of this Act, is liable on conviction to imprisonment for a term of not less than fifteen years without an option of fine.

(2) Where the offence committed under subsection (1) of this section results in grievous bodily injury, the offender shall be liable on conviction to imprisonment for a minimum term of 15 years without option of fine.

(3) Where the offence committed under subsection (1) of this section results in death, the offender shall be liable on conviction to death sentence without out option of fine.

6. Unlawful access to a computer

(1) Any person, who without authorization or in excess of authorization, intentionally accesses in whole or in part, a computer system or network, commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than N5,000,000 or to both fine and imprisonment.

(2) Where the offence provided in subsection (1) of this section is committed with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or confidential information, the punishment shall be imprisonment for a term of not less than three years or a fine of not less than N7,000,000.00 or to both fine and imprisonment.

7. Unlawful interception of communications

Any person, who intentionally and without authorization or in excess of authority, intercepts by technical means, transmissions of non-public computer data, content data or traffic data, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network; commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than N5,000,000.00 or to both fine and imprisonment.

8. Unauthorized modification of computer data

(1) Any person who directly or indirectly does an act without authority and with intent to cause an unauthorized modification of any data held in any computer system or network, commits an offence and liable on conviction to imprisonment for a term of not less than 3 years or to a fine of not less than N7,000,000.00 or to both fine and imprisonment.

(2) Any person who engages in damaging, deletion, deteriorating, alteration, restriction or suppression of data within computer systems or networks, including data transfer from a computer system by any person without authority or in excess of authority, commits an offence and liable on conviction to imprisonment for a term of not less than three years or to a fine of not less than N7,000,000.00 or to both fine and imprisonment.
(3) For the purpose of this section, a modification of any data held in any computer system or network takes place where, by the operation of any function of the computer, computer system or network concerned any-
(i) program or data held in it is altered or erased;
(ii) program or data is added to or removed from any program or data held in it; or
(iii) act occurs which impairs the normal operation of any computer, computer system or network concerned.

9. System interference

Any person who without authority or in excess of authority, intentionally does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference in the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than N5,000,000.00 or to both fine and imprisonment.

10. Misuse of devices

(1) Any person who unlawfully produces, supplies, adapts, manipulates or procures for use, imports, exports, distributes, offers for sale or otherwise makes available-
(a) any devices, including a computer program or a component designed or adapted for the purpose of committing an offence under this Act;

(b) a computer password, access code or similar data by which the whole or any part of a computer, computer system or network is capable of being accessed for the purpose of committing an offence under this Act, or

(c) any device designed primarily to overcome security measures in any computer, computer system or network with the intent that the devices be utilized for the purpose of violating any provision of this Act, commits an offence and is liable on conviction to imprisonment for a term of not less than three years or a fine of not less than N7,000,000.00 or to both imprisonment and fine.
(2) Any person who with intent to commit an offence under this Act, has in his possession any devise or program referred to in subsection (1) of this section, commits an offence and shall be liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than N5,000,000.00 or to both fine and imprisonment.
(3) Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer or network for any unlawful purpose or gain, commits an offence and shall be liable on conviction to

imprisonment for a term of not less than two years or to a fine of not less than N5,000,000.00 or to both fine and imprisonment.
(4) Where the offence under subsection (1) of this section results in substantial loss or damage, the offender shall be liable to imprisonment for a term of not less than five years or to a fine of not less than N10,000,000.00 or to both fine and imprisonment.
(5) Any person who with intent to commit any offence under this Act uses any automated means or device or any computer program or software to retrieve, collect and store password, access code or any means of gaining access to any program, data or database held in any computer, commits an offence and shall be liable on conviction to imprisonment for a term of not less than five years or to a fine of not less than N10,000,000.00 or to both fine and imprisonment.

11. Computer related forgery

Any person who knowingly accesses any computer or network and inputs, alters, deletes or suppresses any data resulting in inauthentic data with the intention that such inauthentic data will be considered or acted upon as if it were authentic or genuine, regardless of whether or not such data is directly readable or intelligible, commits an offence and is liable on conviction to imprisonment for a term of not less than three years or to a fine of not less than N7,000,000.00 or to both fine and imprisonment.

12. Computer related fraud

(1) Any person who knowingly and without authority or in excess of authority causes any loss of property to another by altering, erasing, inputting or suppressing any data held in any computer, whether or not for the purpose of conferring any economic benefits for himself or another person, commits an offence and is liable on conviction to imprisonment for a term of not less than three years or to a fine of not less than N7,000,000.00 or to both fine and imprisonment.
(2) Any person who with intent to defraud sends electronic message to a recipient, where such electronic message materially misrepresents any fact or set of facts upon which reliance the recipient or another person is caused to suffer any damage or loss, commits an offence and shall be liable on conviction to imprisonment for a term of not less than five years or to a fine of not less than N10,000,000.00 or to both fine and imprisonment.

13. Identity theft and impersonation

Any person who in the course of using a computer, computer system or network-
(a) knowingly obtains or possesses another person‘s or entity‘s identity information with the intent to deceive or defraud, or

(b) fraudulently impersonates another entity or person, living or dead, with intent to -
(i) gain advantage for himself or another person;
(ii) obtain any property or an interest in any property;
(iii) cause disadvantage to the entity or person being impersonated or another person; or
(iv) avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice,

commits an offence and liable on conviction to imprisonment for a term of not less than three years or a fine of not less than N7,000,000.00 or to both fine and imprisonment.

14. Child pornography and related offences

(1) Any person who intentionally uses any computer or network system in or for-
(a) producing child pornography for the purpose of its distribution;
(b) offering or making available child pornography;
(c) distributing or transmitting child pornography;
(d) procuring child pornography for oneself or for another person;
(e) possessing child pornography in a computer system or on a computer-data storage medium;
commits an offence under this Act and is liable on conviction –
(i) in the case of paragraphs (a), (b) and (c) to imprisonment for a term of ten years or a fine of not less than N20,000,000.00 or to both fine and imprisonment, and
(ii) in the case of paragraphs (d) and (e) of this subsection, to imprisonment for a term of not less than five years or a fine of not less than N10,000,000.00 or to both fine and imprisonment.

(2) Any person who, intentionally proposes, grooms or solicits, through information and communication technologies, to meet a child, followed by material acts leading to such a meeting for the purpose of:
(a) engaging in sexual activities with a child;
(b) engaging in sexual activities with a child where -
(i) use is made of coercion, inducement, force or threats;
(ii) abuse is made of a recognised position of trust, authority or influence over the child, including within the family; or
(iii) abuse is made of a particularly vulnerable situation of the child, mental or physical disability or a situation of dependence;
(c) recruiting, inducing, coercing, or causing a child to participate in pornographic performances or profiting from or otherwise exploiting a child for such purposes;
commits an offence under this Act and is liable on conviction-
(i) in the case of paragraphs (a) and (b) to imprisonment for a term of not less than 10 years or a fine of not less than N15,000,000 or to both fine and imprisonment; and

(ii) in the case of paragraph (c) of this subsection, to imprisonment for a term of not less than five years or a fine of not less than N10,000,000 or to both fine and imprisonment.
(3) For the purpose of subsection (1) above, the term ~~"c~~hild pornography" shall include pornographic material that visually depicts-
(a) a minor engaged in sexually explicit conduct;
(b) a person appearing to be a minor engaged in sexually explicit conduct; and
(c) realistic images representing a minor engaged in sexually explicit conduct.
(4) For the purpose of this section, the term ~~"c~~hild" or ~~"m~~inor" shall include a person below 18 years of age.

15. Cyberstalking

(1) Any person who, by means of a public electronic communications network persistently sends a message or other matter that -

(a) is grossly offensive or of an indecent, obscene or menacing character or causes any such message or matter to be so sent; or
(b) he knows to be false, for the purpose of causing annoyance, inconvenience or needless anxiety to another or causes such a message to be sent; commits an offence under this Act and shall be liable on conviction to a fine of not less than N2,000,000.00 or imprisonment for a term of not less than one year or to both fine and imprisonment.
(2) Any person who, through information and communication technologies, by means of a public electronic communications network, transmits or causes the transmission of any communication –
(a) with intent to bully, threaten or harass another person, where such communication places another person in fear of death, violence or personal bodily injury or to another person;

(b) containing any threat to kidnap any person or any threat to injure the person of another, any demand or request for a ransom for the release of any kidnapped person, with intent to extort from any person, firm, association or corporation, any money or other thing of value; or

(c) containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, with intent to extort from any person, firm, association, or corporation, any money or other thing of value;

commits an offence under this Act and is liable on conviction-
(i) in the case of paragraphs (a) and (b) of this subsection to imprisonment for a term of not less than ten years or a fine of not less than N25,000,000 or to both fine and imprisonment; and

(ii) in the case of paragraph (c) of this subsection, to imprisonment for a term of not less than five years or a fine of not less than N15,000,000.00 or to both fine and imprisonment.
(3) A court sentencing or otherwise dealing with a person convicted of an offence under subsections (1) and (2) may (as well as sentencing him or dealing with him in any other way) make an order, which may, for the purpose of protecting the victim or victims of the offence, or any other person mentioned in the order, from further conduct which-
(a) amounts to harassment, or
(b) will cause a fear of violence, death or bodily injury; prohibit the defendant from doing anything described/specified in the order.
(4) A defendant who does anything which he is prohibited from doing by an order under this section, commits an offence under this section and shall be liable on conviction to a fine of not less than N10,000,000.00 or imprisonment for a term of not less than three years or to both fine and imprisonment.
(5) The order made under subsection (3) of this section may have effect for a specified period or until further order and the defendant or any other person mentioned in the order may apply to the court which made the order for it to be varied or discharged by a further order.

16. Cybersquatting

(1) Any person who, intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by any individual, body

corporate or belonging to either the Federal, State or Local Governments in Nigeria, on the internet or any other computer network, without authority or right, or for the purpose of interfering with their use by the owner, registrant or legitimate prior user, commits an offence under this Act and is liable on conviction to imprisonment for a term of not less than two years or a fine of not less than N5,000,000.00 or to both fine and imprisonment.

(2) In awarding any penalty against an offender under this section, a court shall have regard to the following -

(a) a refusal by the offender to relinquish, upon formal request by the rightful owner of the name, business name, trademark, domain name, or other word or phrase registered, owned or in use by any individual, body corporate or belonging to either the Federal, State or Local Governments in Nigeria; or

(b) an attempt by the offender to obtain compensation in any form for the release to the rightful owner for use in the Internet of the name, business name, trademark, domain name or other word or phrase registered, owned or in use by any individual, body corporate or belonging to either the Federal, State or Local Government of Nigeria.

(3) In addition to the penalty specified under this section, the court may make an order directing the offender to relinquish such registered name, mark, trademark, domain name, or other word or phrase to the rightful owner.

17. Cyber terrorism

(1) Any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and liable on conviction to life imprisonment.

(2) For the purposes of this section, ~~"t~~errorism" shall have the same meaning under the Terrorism (Prevention) Act, 2011, as amended.

18. Racist and xenophobic offences

(1) Any person who -

(a) distributes or otherwise makes available, any racist and xenophobic material to the public through a computer system or network,

(b) threatens, through a computer system or network, with the commission of a criminal offence -

(i) persons for the reason that they belong to a group, distinguished by race, colour, descent, national or ethnic origin, as well as, religion, if used as a pretext for any of these factors, or

(ii) a group of persons which is distinguished by any of these characteristics;

(c) insults publicly, through a computer system or network -

(i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or

(ii) a group of persons which is distinguished by any of these characteristics; or

(d) distributes or otherwise makes available, through a computer system to the public, material which denies, approves or justifies acts constituting genocide or crimes against humanity, as defined under the Rome Statute of the International Criminal Court, 1998;

commits an offence and shall be liable on conviction to imprisonment for a term of not less than five years or to a fine of not less than N10,000,000.00 or to both fine and imprisonment.

(2) For the purpose of subsection (1) of this section, the term **"**racist and xenophobic material" means any written or printed material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

19. Attempt, conspiracy, aiding and abetting

Any person who -

(a) attempts to commit any offence under this Act; or

(b) does any act preparatory to or in furtherance of the commission of an offence under this Act; or

(c) abets, aids or conspires to commit any offence under this Act,

commits an offence and is liable on conviction to the punishment provided for the principal offence under this Act.

20. Corporate liability

(1) A body corporate that commits an offence under this Act shall be liable on conviction to a fine of not less than N10,000,000.00 and any person who at the time of the commission of the offence was a chief executive officer, director, secretary, manager or other similar officer of the body corporate or was purporting to act in any such capacity shall be liable on conviction to imprisonment for a term of not less than two years or a fine of not less than N5,000,000.00 or to both fine and imprisonment;

(2) Nothing contained in this section shall render any person liable to any punishment where he proves that the offence was committed without his knowledge or that he exercised all due diligence to prevent the commission of the offence.

PART IV - DUTIES OF SERVICE PROVIDERS

21. Records retention and protection of data

(1) A service provider shall keep all traffic data and subscriber information as may be prescribed by the relevant authority for the time being responsible for the regulation of communication services in Nigeria.

(2) A service provider shall, at the request of the relevant authority referred to in subsection (1) of this section or any law enforcement agency -

(a) preserve, hold or retain any traffic data, subscriber information or related content, or

(b) release any information required to be kept under subsection (1) of this section

(3) A law enforcement agency may, through its authorised officer, request for the release of any information in respect of subsection (2) (b) of this section and it shall be the duty of the service provider to comply.

(4) Any data retained, processed or retrieved by the service provider at the request of any law enforcement agency under this Act shall not be utilized except for legitimate purposes as may be provided for under this Act, any other legislation, regulation or by an order of a court of competent jurisdiction.
(5) Anyone exercising any function under this section shall have due regard to the individual's right to privacy under the Constitution of the Federal Republic of Nigeria, 1999 and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved for the purpose of law enforcement.
(6) Subject to the provisions of section 20 of this Act, any person or entity who contravenes any of the provisions of this section commits an offence and is liable on conviction to imprisonment for a term of not less than three year or a fine of not less than N7,000,000.00 or to both fine and imprisonment .

22. Interception of electronic communications

Where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings, a Judge may on the basis of information on oath;
(a) order a service provider, through the application of technical means to collect, record, permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or
(b) authorize a law enforcement officer to collect or record such data through application of technical means.

23. Failure of service provider to perform certain duties.

(1) It shall be the duty of every service provider in Nigeria to comply with all the provisions of this Act and disclose any information requested by any law enforcement agency or otherwise render assistance howsoever in any inquiry or proceeding under this Act.
(2) Without prejudice to the generality of the foregoing, a service provider shall, at the request of any law enforcement agency in Nigeria or at its own initiative, provide assistance towards -
(a) the identification, apprehension and prosecution of offenders;
(b) the identification, tracking and tracing of proceeds of any offence or any property, equipment or device used in the commission of any offence; or
(c) the freezing, removal, erasure or cancellation of the services of the offender which enables the offender to either commit the offence or hide or preserve the proceeds of any offence or any property, equipment or device used in the commission of the offence.
(3) Any service provider who contravenes the provisions of subsection (1) and (2) of this section, commits an offence and shall be liable on conviction to a fine of not less than N10,000,000.00.
(4) In addition to the punishment prescribed under subsection (3) of this section and subject to the provisions of section 20 of this Act, each director, manager or officer of the service provider shall be liable on conviction to imprisonment for a term of not less than three years or a fine of not less than N7,000,000.00 or to both fine and imprisonment.

PART VI - SEARCH, ARREST AND PROSECUTION

27. Power to conduct search and arrest

(1) A law enforcement officer duly authorized may apply *ex-parte* to the court for the issuance of a warrant for the purposes of a cybercrime or computer related crime investigation.

(2) The court may issue a warrant authorizing a law enforcement officer to-

(a) enter the premises or conveyance specified or described in the warrant;

(b) search the premises or conveyance and any person found therein; and

(c) seize and retain any computer or electronic device and relevant material found therein.

(3) The court shall not issue a warrant under subsection (2) of this section unless the court is satisfied that -

(a) the warrant is sought to prevent the commission of an offence under this Act or to prevent the interference with investigative process under this Act; or

(b) for the purpose of investigating cybercrime, cyber-security breach or computer related offences; or

(c) there are reasonable grounds for believing that the person or material on the premises or conveyance may be relevant to the cybercrime or computer related offences under investigation; and

(d) the person named in the warrant is preparing to commit an offence under this Act.

28. Powers to conduct investigation or search without warrant

(1) Where in a case of verifiable urgency, a cybercrime or computer related offences is threatened, or there is the urgent need to prevent the commission of an offence provided under this Act, and an application to the court or to a Judge in Chambers to obtain a warrant would cause delay that may be prejudicial to the maintenance of public safety or order, an authorized law enforcement officer may without prejudice to the provisions of section 27 of this Act or any other law; with the assistance of such other authorized officers as may be necessary and while search warrant is being sought for -

(a) enter and search any premises or place if he has reason to suspect that, within those premises, place or conveyance -

(i) an offence under this Act is being committed or likely to be committed; or

(ii) there is evidence of the commission of an offence under this Act; or

(iii) there is an urgent need to prevent the commission of an offence under this Act

(b) search any person or conveyance found on any premises or place which such authorized officers who are empowered to enter and search under paragraph (a) of this subsection;

(c) stop, board and search any conveyance where the authorised officer has reasons to suspect that there is evidence of the commission or likelihood of the commission of an offence under this Act;

(d) seize, remove and detain anything which is, or contains or appears to him to be or to contain evidence of the commission of an offence under this Act; or

(e) use or cause to use a computer or any device to search any data contained in or available to any computer system or computer network;

(f) use any technology to decode or decrypt any coded or encrypted data contained in a computer into readable text or comprehensible format;

(g) require any person having charge of or otherwise concerned with the operation of any computer or electronic device in connection with an offence under this Act to produce such computer or electronic device; or
(h) arrest, search and detain any person whom the officer reasonably suspects of having committed or likely to commit an offence under this Act.
(2) Where a seizure is effected in the course of search or investigation under this Act, a copy of the list of all the items, documents and other materials seized shall be made, duly endorsed and handed to the-
(a) person on whom the search is made; or
(b) owner of the premises, place or conveyance seized.
(3) Notwithstanding the provisions of subsection (1) of this section, a woman shall only be searched by a woman.
(4) Nothing in this section shall be construed as derogating from the lawful right of any person in defence of his person or property.
(5) A duly authorized law enforcement officer who uses such force as may be reasonably necessary for any purpose in accordance with this Act, shall not be liable in any criminal or civil proceedings, for having, by the use of reasonable force caused injury or death to any person or damage to or loss of any property.

29. Obstruction and refusal to release information.

Any person who –
(a) willfully obstructs any authorized law enforcement officer in the exercise of any powers conferred by this Act; or
(b) fails to comply with any lawful inquiry or requests made by an authorized law enforcement agency in accordance with the provisions of this Act,
commits an offence and shall be liable on conviction to imprisonment for a term of two years or to a fine of not less than N500,000.00 only or to both fine and imprisonment.

30. Prosecution of offences

The Attorney-General of the Federation shall prosecute offences under this Act subject to the provisions of the Constitution of the Federal Republic of Nigeria, 1999.

31. Order of forfeiture of assets.

(1) The Court in imposing sentence on any person convicted of an offence under this Act, may order that the convicted person forfeits to the Government of the Federal Republic of Nigeria –
(a) any asset, money or property, whether tangible or intangible, constituting or traceable to proceeds of such offence; and
(b) any computer, equipment, software or electronic device and other technological device used or intended to be used to commit or to facilitate the commission of such offence;
(2) Where it is established that a convicted person has assets or properties in a foreign country, acquired as a result of such criminal activities listed in this Act, such assets or properties, shall subject to any Treaty or arrangement with such foreign country, be forfeited to the Federal Government of Nigeria.

(4) The office of the Attorney-General of the Federation shall ensure that the forfeited assets or properties are effectively transferred and vested in the Federal Government of Nigeria.

(3) Any person convicted of an offence under this Act shall surrender his International Passport to the Government of the Federal Republic of Nigeria until he has served the sentence or paid the fines imposed on him. (4) Notwithstanding subsection (2) of this section, the President may upon the grant of pardon to the convicted person -
(a) for the purposes of allowing the convicted person to travel abroad for medical treatment; or
(b) in the public interest;
direct that the passport or travel documents of the convicted person be released to him on the recommendation of the Minister.

32. Order for payment of compensation or restitution

Without prejudice to section 31 of this Act, the Court in imposing sentence on any person convicted under this Act may make an Order requiring the convicted person to pay, in addition to any penalty imposed on him under this Act, monetary compensation to any person or entity for any damage, injury or loss caused to his computer, computer system or network, program or data or to recover any money lost or expended by such person or entity as a result of the offence being convicted for.

APPENDIX C (UNITED KINGDOM LEGISLATION)- COMPUTER MISUSE ACT 1990.

1. Unauthorised access to computer material.

(1) A person is guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer , or to enable any such access to be secured ;

(b) the access he intends to secure , or to enable to be secured, is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2)The intent a person has to have to commit an offence under this section need not be directed at

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

2. Unauthorised access with intent to commit or facilitate commission of further offences.

(1) A person is guilty of an offence under this section if he commits an offence under section 1 above (~~"t~~he unauthorised access offence") with intent—

(a) to commit an offence to which this section applies; or

(b) to facilitate the commission of such an offence (whether by himself or by any other person);

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences—

(a) for which the sentence is fixed by law; or

(b) for which a person who has attained the age of twenty-one years (eighteen in relation to England and Wales) and has no previous convictions may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the Magistrates‘ Courts Act 1980).

(3)It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

(5) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

3. Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer,etc.

(1) A person is guilty of an offence if—

(a) he does any unauthorised act in relation to a computer;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) either subsection (2) or subsection (3) below applies.

(2)This subsection applies if the person intends by doing the act—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer;

(c) to impair the operation of any such program or the reliability of any such data; or

(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.

(3)This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.

(4)The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to—

(a) any particular computer;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(5)In this section—

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) ~~a~~act" includes a series of acts;

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

(6) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine or to both.

3A. Making, supplying or obtaining articles for use in offence under section 1 or 3.

(1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3.

(2) A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1 or 3.

(3) A person is guilty of an offence if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1 or 3.

(4) In this section "article" includes any program or data held in electronic form.

(5) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.]

APPENDIX D – 1999 CONSTITUTION OF THE FEDERAL REPUBLIC OF NIGERIA

Chapter I

General Provisions

Part I

Federal Republic of Nigeria

1. (1) This Constitution is supreme and its provisions shall have binding force on the authorities and persons throughout the Federal Republic of Nigeria.

(2) The Federal Republic of Nigeria shall not be governed, nor shall any persons or group of persons take control of the Government of Nigeria or any part thereof, except in accordance with the provisions of this Constitution.

(3) If any other law is inconsistent with the provisions of this Constitution, this Constitution shall prevail, and that other law shall, to the extent of the inconsistency, be void.

2. (1) Nigeria is one indivisible and indissoluble sovereign state to be known by the name of the Federal Republic of Nigeria.

(2) Nigeria shall be a Federation consisting of States and a Federal Capital Territory.

3. (1) There shall be 36 states in Nigeria, that is to say, Abia, Adamawa, Akwa Ibom, Anambra, Bauchi, Bayelsa, Benue, Borno, Cross River, Delta, Ebonyi, Edo, Ekiti, Enugu, Gombe, Imo, Jigawa, Kaduna, Kano, Katsina, Kebbi, Kogi, Kwara, Lagos, Nasarawa, Niger, Ogun, Ondo, Osun, Oyo, Plateau, Rivers, Sokoto, Taraba, Yobe and Zamfara.

(2) Each state of Nigeria, named in the first column of Part I of the First Schedule to this Constitution, shall consist of the area shown opposite thereto in the second column of that Schedule.

(3) The headquarters of the Governor of each State shall be known as the Capital City of that State as shown in the third column of the said Part I of the First Schedule opposite the State named in the first column thereof.

(4) The Federal Capital Territory, Abuja, shall be as defined in Part II of the First Scheduled to this Constitution.

(5) The provisions of this Constitution in Part I of Chapter VIII hereof shall in relation to the Federal Capital Territory, Abuja, have effect in the manner set out thereunder.

(6) There shall be 768 Local Government Areas in Nigeria as shown in the second column of Part I of the First Schedule to this Constitution and six area councils as shown in Part II of that Schedule.